Suvestinė redakcija nuo 2019-04-27

Nutarimas paskelbtas: TAR 2018-08-21, i. k. 2018-13252

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS
DĖL LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO ĮGYVENDINIMO

2018 m. rugpjūčio 13 d. Nr. 818
Vilnius

Pakeistas teisės akto pavadinimas:
Nr. 1209, 2018-12-05, paskelbta TAR 2018-12-10, i. k. 2018-20153

Vadovaudamasi Lietuvos Respublikos kibernetinio saugumo įstatymo 5 straipsnio 1–5 punktais ir įgyvendindama 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL 2016 L 194, p. 1), Lietuvos Respublikos Vyriausybė n u t a r i a:
Preambulės pakeitimai:
Nr. 1209, 2018-12-05, paskelbta TAR 2018-12-10, i. k. 2018-20153
Nr. 390, 2019-04-24, paskelbta TAR 2019-04-26, i. k. 2019-06920

1. Patvirtinti pridedamus:

1.1. Nacionalinę kibernetinio saugumo strategiją;

1.2. Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką (toliau – Metodika);

1.3. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašą (toliau – Aprašas);

1.4. Nacionalinį kibernetinių incidentų valdymo planą (toliau – Planas).
Punkto pakeitimai:
Nr. 1209, 2018-12-05, paskelbta TAR 2018-12-10, i. k. 2018-20153

2. Pavesti Lietuvos Respublikos krašto apsaugos ministerijai iki 2018 m. lapkričio 2 d. pateikti Lietuvos Respublikos Vyriausybei tvirtinti Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinį veiklos plano projektą.

3. Pasiūlyti:

3.1. nevyriausybinėms organizacijoms, suinteresuotiems viešojo ir privataus sektorių atstovams, Lietuvos mokslo ir studijų institucijoms dalyvauti įgyvendinant Nacionalinę kibernetinio saugumo strategiją;

3.2. Lietuvos Respublikos Prezidento kanceliarijai, Lietuvos Respublikos Seimo kanceliarijai, Lietuvos Respublikos vyriausiajai rinkimų komisijai, Lietuvos vyriausiojo archyvaro tarnybai Metodikos nustatyta tvarka nustatyti visus jų veiklos srityje veikiančius infrastruktūros objektus, turinčius reikšmės teikiant ypatingos svarbos paslaugas valstybės valdymo sektoriuje, užpildyti Metodikos 2 priede pateiktą klausimyną, jį pateikti Metodikos 1 priede nurodytai institucijai (institucijoms) ir Metodikos nustatyta tvarka vykdyti Atsakingo valdytojo funkcijas;

3.3. Lietuvos Respublikos generalinei prokuratūrai, Nacionalinei teismų administracijai, Lietuvos Respublikos specialiųjų tyrimų tarnybai Metodikos nustatyta tvarka nustatyti visus jų veiklos srityje veikiančius infrastruktūros objektus, turinčius reikšmės teikiant ypatingos svarbos paslaugas valstybės valdymo bei viešojo saugumo ir teisinės tvarkos sektoriuose, užpildyti Metodikos 2 priede pateiktą klausimyną, jį pateikti Metodikos 1 priede nurodytai institucijai (institucijoms) ir Metodikos nustatyta tvarka vykdyti Atsakingo valdytojo funkcijas;

3.4. Lietuvos Respublikos ryšių reguliavimo tarnybai pagal kompetenciją bendradarbiauti su Lietuvos Respublikos susisiekimo ministerija ir teikti būtina ekspertinę pagalbą jai atliekant Metodikoje nurodytas Atsakingos institucijos funkcijas informacinių technologijų ir elektroninių ryšių sektoriaus elektroninių ryšių subsektoriuje;

3.5. Lietuvos Respublikos savivaldybių administracijoms Metodikos nustatyta tvarka nustatyti visus jų veiklos srityje veikiančius infrastruktūros objektus, turinčius reikšmės teikiant ypatingos svarbos paslaugas energetikos, transporto ir pašto, sveikatos priežiūros, geriamojo vandens tiekimo, paskirstymo ir tvarkymo, valstybės valdymo sektoriuose, užpildyti Metodikos 2 priede pateiktą klausimyną, jį pateikti Metodikos 1 priede nurodytai institucijai (institucijoms) ir Metodikos nustatyta tvarka vykdyti Atsakingo valdytojo funkcijas;

3.6. Lietuvos bankui 2.3 papunktyje nustatyta tvarka paskirti atsakingus asmenis ir šio nutarimo bei Metodikos nustatyta tvarka vykdyti Metodikos 1 priede nurodytų institucijų funkcijas finansų sektoriuje;

3.7 institucijoms, nurodytoms Plano 5 punkte, išskyrus Lietuvos Respublikos krašto apsaugos ministeriją, paskirti asmenis, atsakingus už informacijos perdavimą pagal Plane nustatytą tvarką, ir pateikti šių asmenų kontaktinę informaciją Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos.

Punkto pakeitimai:
Nr. 1209, 2018-12-05, paskelbta TAR 2018-12-10, i. k. 2018-20153

4. Pavesti:

4.1. institucijoms, nurodytoms Metodikos 1 priede, iki 2019 m. vasario 1 d. Metodikos nustatyta tvarka inicijuoti ypatingos svarbos infrastruktūros objektų peržiūrą ir kreiptis į institucijas, įstaigas, įmones ar jos struktūrinius padalinius, kurie yra infrastruktūros objektai, ar į infrastruktūros objekto valdytojus, kai infrastruktūros objektas yra įrenginys ar įrenginio dalis (toliau – Atsakingas valdytojas), prašant Atsakingų valdytojų atlikti visų jų valdomų infrastruktūros objektų svarbos vertinimą ir užpildyti Metodikos 2 priede pateiktą klausimyną;

4.2. institucijoms, nurodytoms Metodikos 1 priede, iki 2019 m. vasario 1 d. paskirti asmenis, atsakingus už ypatingos svarbos sektoriuose veikiančių ir ypatingos svarbos paslaugas teikiančių ypatingos svarbos infrastruktūros objektų nustatymą ir ypatingos svarbos informacinės infrastruktūros identifikavimą, ir pateikti šių asmenų kontaktinę informaciją Krašto apsaugos ministerijai;

4.3. Krašto apsaugos ministerijai iki 2019 m. vasario 1 d. paskirti asmenis, atsakingus už informacijos perdavimą pagal Plane nustatytą tvarką, ir pateikti šių asmenų kontaktinę informaciją Nacionaliniam kibernetinio saugumo centrui;

4.4. institucijoms, nurodytoms Plano 4 punkte, iki 2019 m. vasario 1 d. paskirti asmenis, su kuriais būtų galima susisiekti visą parą ir kurie būtų atsakingi už keitimąsi informacija kibernetinio incidento valdymo metu, numatyti šių asmenų pakeičiamumą, o Valstybinei duomenų apsaugos inspekcijai ir Lietuvos policijai pateikti šių asmenų kontaktinę informaciją Nacionaliniam kibernetinio saugumo centrui;

4.5. kibernetinio saugumo subjektams iki 2019 m. vasario 1 d. paskirti atsakingus asmenis, su kuriais galima susisiekti visą parą, ir pateikti šių asmenų telefono numerius, elektroninio pašto adresus, kitą kontaktinę informaciją, sudarančią sąlygas visą parą keistis

informacija kibernetinio incidento valdymo metu, Nacionaliniam kibernetinio saugumo centrui.

Papildyta punktu:
Nr. 1209, 2018-12-05, paskelbta TAR 2018-12-10, i. k. 2018-20153

5. Patvirtinti Kibernetinio saugumo tarybos (toliau – Taryba) institucinę sudėtį:

Lietuvos Respublikos krašto apsaugos ministerijos atstovai (du asmenys);

Lietuvos Respublikos Vyriausybės kanceliarijos atstovas;

Lietuvos Respublikos ekonomikos ir inovacijų ministerijos atstovas;

Lietuvos Respublikos energetikos ministerijos atstovas;

Lietuvos Respublikos susisiekimo ministerijos atstovas;

Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos atstovas;

Lietuvos Respublikos teisingumo ministerijos atstovas;

Lietuvos Respublikos užsienio reikalų ministerijos atstovas;

Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos atstovas;

Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos atstovas;

Valstybinės duomenų apsaugos inspekcijos atstovas;

Policijos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos atstovas;

Lietuvos Respublikos ryšių reguliavimo tarnybos atstovas;

Lietuvos banko atstovas;

Lietuvos bankų asociacijos atstovas;

Kauno technologijos universiteto atstovas;

Vilniaus universiteto atstovas;

asociacijos „Infobalt“ atstovai (trys asmenys);

Interneto žiniasklaidos asociacijos atstovas;

Lietuvos savivaldybių asociacijos atstovas;

Lietuvos šilumos tiekėjų asociacijos atstovas;

Lietuvos vandens tiekėjų asociacijos atstovas;

„Lietuvos energija“, UAB, atstovas;

„EPSO-G“, UAB, atstovas.

Papildyta punktu:
Nr. 390, 2019-04-24, paskelbta TAR 2019-04-26, i. k. 2019-06920

Ministras Pirmininkas Saulius Skvernelis

Krašto apsaugos ministras Raimundas Karoblis

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2018 m. rugpjūčio 13 d. nutarimu Nr. 818

NACIONALINĖ KIBERNETINIO SAUGUMO STRATEGIJA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinė kibernetinio saugumo strategija (toliau – Strategija) nustato svarbiausias nacionalinės kibernetinio saugumo politikos viešajame ir privačiame sektoriuose kryptis. Įgyvendinant Strategiją siekiama stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą, užtikrinti nusikalstamų veikų, kurias vykdant naudojami kibernetinę erdvę sudarantys objektai (toliau – nusikalstamos veikos kibernetinėje erdvėje), prevenciją, užkardymą ir tyrimą, skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą, stiprinti glaudų viešojo ir privataus sektorių, tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą valstybėje iki 2023 m.

2. Strategija parengta atsižvelgiant į aplinkos analizę, atliktų tyrimų duomenis, viešojo ir privataus sektorių atstovų pasiūlymus ir atitinka Septynioliktosios Lietuvos Respublikos Vyriausybės programos, kuriai pritarta Lietuvos Respublikos Seimo 2016 m. gruodžio 13 d. nutarimu Nr. XIII-82 „Dėl Lietuvos Respublikos Vyriausybės programos“ (toliau – Lietuvos Respublikos Vyriausybės programa), Nacionalinio saugumo strategijos, patvirtintos Lietuvos Respublikos Seimo 2002 m. gegužės 28 d. nutarimu Nr. IX-907 „Dėl Nacionalinio saugumo strategijos patvirtinimo“, Lietuvos Respublikos kibernetinio saugumo įstatymo, Europos Parlamento, Tarybos, Europos Komisijos komunikatų ir rekomendacijų kibernetinio saugumo srityje, taip pat Europos Komisijos 2015 m. gegužės 6 d. komunikato Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui „Europos skaitmeninės rinkos strategija“ ir Informacinės visuomenės plėtros 2014–2020 metų programos „Lietuvos Respublikos skaitmeninė darbotvarkė“, patvirtintos Lietuvos Respublikos Vyriausybės 2014 m. kovo 12 d. nutarimu Nr. 244 „Dėl Informacinės visuomenės plėtros 2014–2020 metų programos „Lietuvos Respublikos skaitmeninė darbotvarkė“ patvirtinimo“, nuostatas. Lietuvai tapus visaverte Europos ekonominio bendradarbiavimo ir plėtros organizacijos nare, šios organizacijos rekomendacijos dėl skaitmeninės rizikos valdymo, ekonominio ir socialinio klestėjimo taip pat yra viena iš svarbių gairių, kuriomis paremta Strategija.

3. Strategijoje vartojamos sąvokos atitinka Kibernetinio saugumo įstatyme, Lietuvos Respublikos krašto apsaugos sistemos organizavimo ir karo tarnybos įstatyme, Lietuvos Respublikos mokslo ir studijų įstatyme, Lietuvos Respublikos teisės gauti informaciją iš valstybės ir savivaldybių institucijų ir įstaigų įstatyme apibrėžtas sąvokas.

II SKYRIUS
STRATEGIJOS TIKSLAI, UŽDAVINIAI, VERTINIMO KRITERIJAI IR JŲ REIKŠMĖS

4. Strategijos pagrindinis tikslas – efektyviai ir laiku identifikuojant kibernetinius incidentus, užkertant kelią jų atsiradimui ir plitimui, valdant kibernetinių incidentų sukeltas pasekmes, užtikrinti galimybę Lietuvos visuomenei saugiai naudotis informacinių ir ryšių technologijų (toliau – IRT) teikiamomis galimybėmis.

PIRMASIS SKIRSNIS

VALSTYBĖS KIBERNETINIS SAUGUMAS IR KIBERNETINIAI GYNYBOS PAJĖGUMAI

5. **Pirmasis Strategijos tikslas** – stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą.

6. Lietuva, kaip ir kitos pasaulio valstybės, kuriose aktyviai naudojamasi IRT teikiamomis galimybėmis, turinčios puikiai išplėtotą plačiajuosčio ryšio infrastruktūrą, tampa patraukli ne tik pavieniams asmenims, jų grupuotėms ar organizuotoms grupėms, bet ir Lietuvos Respublikos valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie Lietuvos Respublikos krašto apsaugos ministerijos (toliau – VSD ir AOTD) rengiamose kasmetinėse Grėsmių nacionaliniam saugumui vertinimo ataskaitose įvardytoms valstybėms, keliančioms grėsmę Lietuvos nacionaliniam saugumui ir vykdančioms priešišką veiklą pasaulio ir Lietuvos kibernetinėje erdvėje. Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC), VSD ir AOTD surinkti duomenys rodo, kad Lietuva nuolat susiduria su įvairaus tipo kibernetiniais incidentais, skirtais valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai pažeisti; prognozuojama, kad ateityje jų skaičius ir mastas nemažės[1].

7. 2017 m. Nacionalinio kibernetinio saugumo būklės ataskaitos duomenimis, 2017 m. Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apdorojo 54 414 kibernetinius incidentus. 2017 m. kibernetinių incidentų užregistruota dešimtadaliu daugiau nei 2016 m. Lietuvos valstybės informaciniai ištekliai tebėra prioritetinis kibernetinio šnipinėjimo taikinys, bet taikomasi ir į privataus sektoriaus ypatingos svarbos informacinę infrastruktūrą, kitas įmones, turinčias strateginę ar svarbią reikšmę nacionaliniam saugumui. NKSC, taikydamas technines kibernetinio saugumo priemones, daugiausiai kenkimo programinės įrangos paplitimo atvejų nustatė energetikos (27 proc.), viešojo saugumo ir teisinės tvarkos (22 proc.) bei užsienio reikalų ir saugumo politikos (21 proc.) sektoriuose. Palyginti su 2016 m., kenkimo programinė įranga labiau plito viešojo saugumo ir teisinės tvarkos, užsienio reikalų ir saugumo politikos, energetikos sektoriuose. Šalies kibernetinio saugumo situacijai įtaką daro ir viešojo sektoriaus interneto svetainių būklė, kuri, 2017 m. Nacionalinio kibernetinio saugumo būklės ataskaitos duomenimis, 2017 m. pablogėjo.

8. NKSC, VSD ir AOTD kasmetinėse ataskaitose pateikiama informacija apie kibernetinių incidentų paplitimo mastą rodo, kad kiekvienas kibernetinio saugumo subjektas susiduria su situacija, kai reikia spręsti, kiek laiko, pinigų ar kitų išteklių gali prireikti turimų ryšių ir informacinių sistemų ar teikiamų paslaugų apsaugai. Kibernetinio saugumo subjektai atlieka saugumo rizikos vertinimą, bet rizikos vertinimas dažnai atliekamas formaliai, siekiant atitikti teisės aktų reikalavimus ar tarptautiniu mastu pripažintų standartų nuostatas.

Prieš dvylika metų Lietuvos Respublikos vidaus reikalų ministerijos išleista metodinė priemonė „Rizikos analizės vadovas“ atspindi to laiko rizikos vertinimo mokslo ir inovacijų pažangą, tačiau saugumo rizikos vertinimo metodikos nuostatos ilgainiui kito ir iš kontrolės aplinkos užtikrinimo buvo pereita į visa apimantį organizacijos veiklos rizikos vertinimą.

9. Lietuvoje pavieniai įvairių saugumo sričių rizikos vertinimo procesai jau pasiekė brandą, tačiau nacionaliniu lygiu saugumo rizikos vertinimo kultūra, kibernetinio saugumo rizikos vertinimas tebėra fragmentiškas. Trūksta kibernetinių grėsmių ir saugumo spragų analizės visapusės integracijos į veiklos rizikos vertinimo procesus, o sparčiai plėtojantis IRT už kibernetinį saugumą atsakingam personalui pradeda trūkti rizikos vertinimo žinių, gebėjimų ir praktikos.

---

[1] Lietuvos Respublikos valstybės saugumo departamentas ir Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos (2018). *Grėsmių nacionaliniam saugumui vertinimas*; Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (2018). *2017 m. Nacionalinio kibernetinio saugumo būklės ataskaita.*

10. Siekiant tobulinti kibernetinio saugumo politikos formavimo ir įgyvendinimo kultūrą, atnaujinti kibernetinio saugumo rizikos vertinimo ir kitus reikalavimus, 2018 m. kibernetinio saugumo srityje įvyko šie reikšmingi pokyčiai:

10.1. Nauja redakcija išdėstytos Kibernetinio saugumo įstatymo nuostatos patobulino kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, patikslino kibernetinio saugumo politiką formuojančių ir įgyvendinančių institucijų kompetenciją, funkcijas, teises ir pareigas, kibernetinio saugumo subjektų pareigas bei atsakomybę ir nustatė papildomas kibernetinio saugumo užtikrinimo priemones.

10.2. Buvo sutelktos valstybės informacinių išteklių saugumo, viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veiklos reguliavimo ir saugumo funkcijos, o tai leidžia valstybėje užtikrinti sistemingą kibernetinės erdvės stebėjimą, kibernetinių incidentų kibernetinio saugumo subjektų ryšių ir informacinėse sistemose valdymą ir atsakomybę; NKSC tapo vienintele Lietuvos institucija, organizuojančia kibernetinių incidentų valdymą šalyje ir vieno langelio principu teikiančia pagalbą valstybės institucijoms, verslui ir gyventojams.

11. Konsoliduojant pajėgumus, Lietuvoje siekiama kurti integralią kibernetinio saugumo vadybos sistemą, kuri įprasmintų sisteminį požiūrį į bet kurios srities saugumo vadybos planavimą, skatintų kibernetinio saugumo subjektų orientaciją į saugumo vadybos kokybės užtikrinimą, mažintų administracinę naštą kibernetinio saugumo subjektams, užtikrintų vertinimo sistemiškumą ir įrodymais pagrįstą saugumo valdymo kultūrą, padėtų optimizuoti saugumo išlaidų planavimą. Taip pat siekiama užtikrinti tolygią kibernetinio saugumo kompetencijų plėtrą ir regioninių kibernetinio saugumo pajėgumų stiprinimą.

12. Lietuvos Respublikos krašto apsaugos ministerija ir NKSC nuolat bendrauja su kibernetinio saugumo subjektais ir teikia konsultacijas kibernetinio saugumo tematika, rengia kibernetinio saugumo pratybas.

2017 m. nacionalinėse kibernetinio saugumo pratybose „Kibernetinis skydas 2017“ dalyvavo apie 200 dalyvių iš daugiau nei 50 viešojo ir privataus sektorių organizacijų. Bendradarbiaujant su Lietuvos Respublikos ryšių reguliavimo tarnyba, Lietuvos policija ir Valstybine duomenų apsaugos inspekcija, pratybose dalyvaujančių kibernetinio saugumo subjektų atstovams surengti seminarai – supažindinta su kibernetinio saugumo srities teisės aktų reikalavimais. Pratybų dalyviai treniravosi suvaldyti ir atremti kibernetines atakas prieš ypatingos svarbos ryšių ir informacines sistemas ir užtikrinti šių sistemų funkcionavimą.

Krašto apsaugos ministerija ir toliau periodiškai rengs kompleksines nacionalines kibernetinio saugumo pratybas, skatins nuolatinį kibernetinio saugumo įgūdžių tobulinimą ne tik nacionalinėse, bet ir tarptautinėse kibernetinio saugumo pratybose.

13. Europos Sąjunga ir Šiaurės Atlanto sutarties organizacija (toliau – NATO) pripažįsta, kad kibernetinė erdvė pradedama naudoti kaip atskira karo erdvė arba kaip viena iš hibridinio karo priemonių. Kibernetinėmis priemonėmis jau galima sabotuoti valstybės ypatingos svarbos informacinės infrastruktūros veiklą (pvz., 2010 m. įvykdyta kibernetinė ataka Irano branduolinės energetikos objekte), neigiamai paveikti valstybės ir visuomenės saugumą (pvz., 2015 ir 2016 m. kibernetinės atakos Ukrainos elektros jėgainėse), ekonomiką ir socialinę gerovę, todėl nacionalinės kibernetinės erdvės saugumas yra kiekvienos valstybės nacionalinio saugumo interesas.

Pagal 2016 m. NATO viršūnių susitikimo Varšuvoje priimtą sprendimą dėl kibernetinės erdvės pripažinimo penktuoju kariavimo domenu Lietuvos kariuomenė tapo pagrindiniu Lietuvos Respublikos kibernetinės erdvės gynybos subjektu. Kibernetinės gynybos stiprinimas siekiant apsisaugoti nuo besivystančių karinių kibernetinių grėsmių ir efektyvus kibernetinių incidentų valdymas yra viena iš būtinų sąlygų užtikrinant gyvybinius ir pirmaeilius valstybės nacionalinio saugumo interesus. Įgyvendinant Lietuvos kariuomenei keliamus uždavinius, bus plėtojami nacionaliniai kibernetinės gynybos pajėgumai, užtikrinantys Lietuvos kariuomenės sąveiką su valstybės civiliniais pajėgumais, taip pat Lietuvos kariuomenės gebėjimai užtikrinti

patikimą agresorių atgrasymą kibernetinėje erdvėje, o nepavykus atgrasyti – savarankiškai ir kartu su sąjungininkais ginti Lietuvos Respubliką karinėmis kibernetinio saugumo priemonėmis.

14. **Uždaviniai pirmajam Strategijos tikslui pasiekti:**

14.1. *Pirmasis pirmojo tikslo uždavinys* – kurti sisteminį požiūrį į kibernetinį saugumą ir prevencinę veiklą. Šis uždavinys bus įgyvendinamas tobulinant kibernetinio saugumo rizikos nustatymo, vertinimo ir prognozavimo būdus, formuojant kibernetinio saugumo atpažinties paveikslą ir rizikos žemėlapį, kuris atskleistų atskiriems sektoriams būdingas rizikas, kuriant regioninį kibernetinio saugumo centrą ir valstybės valdomą elektroninių ryšių tinklą su kompleksinėmis kibernetinio saugumo priemonėmis, jungiantį valstybines mobilizacines užduotis gyvybiškai svarbioms valstybės funkcijoms atlikti paskirtas vykdyti valstybės ir savivaldybių institucijas, įstaigas ir įmones, atliekant kibernetinio saugumo būsenos tyrimus, pažangos matavimus ar brandos vertinimus, užtikrinant visuomenės informavimą apie kibernetinio saugumo būklę, vykdant kitas kibernetinį saugumą ir prevencinę veiklą stiprinančias priemones ir veiksmus.

14.2. *Antrasis pirmojo tikslo uždavinys* – didinti kibernetinio saugumo politikos formavimo ir įgyvendinimo efektyvumą, mažinant administracinę naštą kibernetinio saugumo subjektams. Šis uždavinys bus įgyvendinamas tobulinant kibernetinio saugumo teisinį reguliavimą, parengiant standartizuotus, bet diferencijuojamus kibernetinio saugumo reikalavimus, atliekant gerosios praktikos, standartų, taikomų užtikrinant kibernetinį saugumą, analizę, skatinant kibernetinio saugumo subjektus jais vadovautis, nustatant nacionalinį integruotą krizių valdymo mechanizmą, užtikrinant visų lygmenų struktūrų sklandų bendradarbiavimą, atnaujinant kibernetinio saugumo rizikos vertinimo sistemą, įvertinant metodines galimybes vykdyti kibernetiniam saugumui reikalingų lėšų stebėseną ir kontrolę, nustatant jų skyrimo ir naudojimo pirmumą, vykdant kitas kibernetinio saugumo politikos formavimo ir įgyvendinimo plėtojimo priemones.

14.3. *Trečiasis pirmojo tikslo uždavinys* – skatinti nacionalinių pratybų vykdymą ir dalyvavimą tarptautinėse pratybose. Šis uždavinys bus įgyvendinamas periodiškai rengiant kompleksines nacionalines kibernetinio saugumo pratybas, dalyvaujant Europos Sąjungos, NATO ir kitų šalių organizuojamose pratybose, integruojant nacionalinių ir tarptautinių pratybų patirtį atliekant situacijų valdymo, incidentų vertinimo, informacijos komunikavimo ar kitus veiksmus.

14.4. *Ketvirtasis pirmojo tikslo uždavinys* – plėtoti valstybės kibernetinės gynybos pajėgumus. Šis uždavinys bus įgyvendinamas užtikrinant efektyvią Lietuvos kariuomenės sąveiką su valstybės civiliniais pajėgumais, plėtojant kibernetinės gynybos pajėgumus ir teikiant pagalbą kitoms valstybės ir savivaldybių institucijoms ir įstaigoms.

ANTRASIS SKIRSNIS
NUSIKALSTAMOS VEIKOS KIBERNETINĖJE ERDVĖJE

15. **Antrasis Strategijos tikslas** – užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą.

16. Nusikalstamos veikos kibernetinėje erdvėje daro didelį neigiamą poveikį pasaulio ekonomikai. Tyrimų duomenimis[2], pasaulinė nusikalstamų veikų kibernetinėje erdvėje padaryta žala siekia šimtus milijardų eurų per metus ir numatoma jos augimo tendencija. Nusikalstamas veikas darančius asmenis domina ne tik finansiniai, bet visi duomenys apskritai, todėl nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui, nurodytų Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje, skaičius nuolat didėja (Nusikalstamų veikų žinybinio registro duomenimis, 2017 m. kibernetinėje erdvėje registruota 594 tokios nusikalstamos veikos, 2016 m. – 336). Europos policijos biure (toliau – Europolas) veikiančio

[2] Center for Strategic and International Studies, „McAfee“ (2018). *Economic Impact of Cybercrime – no slowing down,* Cybersecurity Ventures, Herjavec Group (2017). *2017 Cybercrime Report.*

Europos kovos su elektroniniu nusikalstamumu centro (EC3) teigimu, su nusikalstamomis veikomis kibernetinėje erdvėje dažniausiai susiduria tos Europos Sąjungos valstybės, kuriose gerai išvystyta plačiajuosčio ryšio infrastruktūra ir veikia mokėjimo internetu sistemos[3].

17. „PwC“ kompanijos 2018 m. atlikto Pasaulio ekonominių nusikaltimų tyrimo (*Global Economic Crime Survey 2018*) duomenimis, 2018 m. sukčiavimo nusikaltimai kibernetinėje erdvėje buvo vieni iš dažniausių nusikaltimų, darančių didžiausią žalą privačiam sektoriui. Europole veikiantis Europos kovos su elektroniniu nusikalstamumu centras (EC3) prognozuoja, kad sparčiai vystantis IRT, socialinės inžinerijos metodams ir dėl kitų priežasčių nusikalstamų veikų kibernetinėje erdvėje skaičius vis didės. Be to, į kibernetinę erdvę persikelia vis daugiau nusikalstamų veikų, kurioms atlikti paprastai nebūtina naudoti IRT, pavyzdžiui, sukčiavimas, turto prievartavimas. Joms vykdyti ar pėdsakams slėpti pasitelkiami naujausi IRT sprendimai, kriptovaliutos, naudojamasi anoniminiame tinkle siūlomomis nusikalstamomis paslaugomis.

18. „Cybersecurity Ventures“ kompanija 2017 m. apskaičiavo, kad nusikalstamų veikų kibernetinėje erdvėje, kai naudojama kenkimo programinė įranga, daroma žala kasmet didėja, ir prognozuoja, kad pasaulis iki 2019 m. dėl išpirkos reikalaujančios kenkimo programinės įrangos plitimo patirs daugiau nei vienuolika milijardų dolerių vertės žalos. Europole veikiantis Europos kovos su elektroniniu nusikalstamumu centras (EC3) prognozuoja, kad ši žala ir toliau augs, ypač daugėjant daiktų interneto įrenginių *(Internet of Things (IoT)*. Nors kenkimo programinė įranga dažnai yra tik viena iš priemonių nusikalstamoms veikoms kibernetinėje erdvėje vykdyti, bet Europos tinklų ir saugumo agentūra (ENISA) 2018 m. paskelbtoje 2017 m. grėsmių paplitimo ataskaitoje *(ENISA Threat Landscape Report 2017)* šią kenkimo programinę įrangą jau kelerius metus iš eilės nurodo kaip dažniausią kibernetinę grėsmę.

19. Nusikalstamos veikos, susijusios su vaikų seksualiniu išnaudojimu kibernetinėje erdvėje, laikomos vienomis iš žalingiausių nusikalstamų veikų, kurioms plisti padeda sparčiai besivystančios IRT ir didėjančios naudojimosi jomis galimybės. Šios nusikalstamos veikos kibernetinėje erdvėje įgauna platesnį ir kompleksinį mastą ir jų skaičius, Nusikalstamų veikų žinybinio registro ir Europolo duomenimis, Lietuvoje[4] ir Europoje[5] auga. Lietuva, siekdama užkardyti nusikalstamas veikas, susijusias su vaikų seksualiniu išnaudojimu kibernetinėje erdvėje, perkėlė 2011 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyvą 2011/92/ES dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija, kuria pakeičiamas Tarybos pamatinis sprendimas 2004/68/TVR (OL 2011 L 335, p. 1), ir 2012 m. lapkričio 6 d. ratifikavo Europos Tarybos 2007 m. spalio 25 d. konvenciją dėl vaikų apsaugos nuo seksualinio išnaudojimo ir seksualinės prievartos prieš juos (*Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*).

20. Siekiant užkardyti nusikalstamas veikas kibernetinėje erdvėje, peržengiančias valstybių sienas, svarbu plėtoti glaudų tarpvalstybinį bendradarbiavimą ir keitimąsi informacija, palaikyti ir gilinti santykius, pagrįstus tarptautiniais susitarimais ir naryste. Siekiant šio tikslo itin svarbi stipri politinė valia efektyviai vykdyti tarptautinius įsipareigojimus ir laikytis tarptautinių standartų užtikrinant kibernetinį saugumą ir kovojant su nusikalstamomis veikomis kibernetinėje erdvėje. Išreikšdama tokią politinę valią, Lietuva ratifikavo Europos Tarybos 2001 m. lapkričio 23 d. konvenciją dėl elektroninių nusikaltimų (*Convention on Cybercrime*) (toliau – Budapešto konvencija) ir jos papildomus protokolus. Lietuva taip pat perkėlė 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyvą 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL 2013 L 218, p. 8). Įsipareigojimai sėkmingai vykdomi ne tik teisiniu, bet ir praktiniu lygiu, bendradarbiaujant su Tarptautine kriminalinės policijos organizacija (toliau – Interpolas) ir Interpolo pasauliniu inovacijų kompleksu, Europolu ir jame veikiančiu Europos kovos su elektroniniu

[3] Europol's European Cybercrime Centre (EC3) (2017). *2017 Internet Organised Crime Threat Assessment (IOCTA)*

[4] Nusikalstamų veikų žinybinio registro duomenimis, 2016 m. buvo užregistruoti 123 nusikaltimai pagal Baudžiamojo kodekso 309 str. 2 d., 2017 m. – 132.

[5] European Union Agency for Law Enforcement Cooperation (Europol) (2017). *Europol Review 2016–2017.*

nusikalstamumu centru (EC3) bei Europos teisminio bendradarbiavimo padaliniu (Eurojustas). Taip pat Lietuva dalyvauja nepertraukiamai veikiančių kontaktinių punktų kibernetinių nusikalstamų veikų tyrimo srityje tinklo, įsteigto remiantis Europos teisminiu tinklu (EJN) ir Budapešto konvencija, veikloje.

21. Nusikalstamoms veikoms kibernetinėje erdvėje nuolat evoliucionuojant, įgaunant naujų formų, teisėsaugos institucijų personalas, dirbantis šių nusikalstamų veikų tyrimo ir prevencijos srityje, turi būti tinkamai pasiruošęs įvertinti kibernetines grėsmes, identifikuoti nusikalstamas veikas kibernetinėje erdvėje ir efektyviai jas tirti. Labai svarbi ir tinkama prokuratūros, teismų darbuotojų ir šią veiklą organizuojančių ir jai vadovaujančių vadovų kompetencija. Tiriant šias veikas itin svarbūs teisėsaugos įstaigų gebėjimai surasti, užfiksuoti ir greitai ištirti elektroninius įrodymus.

22. **Uždaviniai antrajam Strategijos tikslui pasiekti**:

22.1. *Pirmasis antrojo tikslo uždavinys* – plėtoti valstybės pajėgumus ir gebėjimus kovoti su nusikalstamomis veikomis kibernetinėje erdvėje. Šis uždavinys bus įgyvendinamas tobulinant teisinę sistemą, stiprinant teisėsaugos institucijų profesinius gebėjimus tirti nusikalstamas veikas kibernetinėje erdvėje, kuriant analizės sistemas, diegiant pažangius veiklos metodus ir procedūras, techninius įrankius, skirtus kovai su nusikalstamomis veikomis kibernetinėje erdvėje.

22.2. *Antrasis antrojo tikslo uždavinys* – stiprinti nusikalstamų veikų kibernetinėje erdvėje prevenciją ir kontrolę. Šis uždavinys bus įgyvendinamas propaguojant visuomenės savisaugos kultūrą ir atsakingą elgesį kibernetinėje erdvėje, tobulinant teisėsaugos institucijų kovos su nusikalstamomis veikomis kibernetinėje erdvėje funkcijų vykdymą ir užtikrinant operatyvesnį tarptautinį bendradarbiavimą tiriant šias nusikalstamas veikas, plėtojant teisėsaugos institucijų efektyvų bendradarbiavimą su mokslo ir studijų institucijomis, viešojo ir privataus sektorių atstovais bei visuomene.

TREČIASIS SKIRSNIS
KIBERNETINIO SAUGUMO KULTŪRA IR INOVACIJOS

23. **Trečiasis Strategijos tikslas** – skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą.

24. Kibernetiniai incidentai šiuolaikiniame pasaulyje yra neišvengiami, nuo jų negalima apsisaugoti net ir taikant visas esamas technines kibernetinio saugumo priemones, todėl viešojo ir privataus sektorių atstovai turi rūpintis savo darbuotojų kibernetinės kultūros kėlimu. IBM kompanijos 2017 m. atlikto tyrimo[6] duomenimis, daugėja kibernetinių incidentų, kurie buvo sukelti per tiriamo privataus sektoriaus darbuotojų aplaidumą ar nežinojimą (2017 m. tokie kibernetiniai incidentai sudarė daugiau nei 20 proc., 2016 m. – 15 proc.). Daugiau nei trečdalis tokių kibernetinių incidentų įvyko, nes darbuotojai atvėrė teisės pažeidėjų atsiųstas nuorodas ar su elektroniniu laišku atsiųstus dokumentus. Lietuvoje taip pat daugėja elektroninių laiškų, sukurtų taikant socialinės inžinerijos metodus[7].

25. 2018 m. Europos inovacijų diegimo rezultatų suvestinės duomenimis, Europoje privataus sektoriaus atstovai vis daugiau dėmesio skiria darbuotojų IRT srities mokymams, tačiau Lietuvoje šis rodiklis tik truputį viršija 10 proc. (rodiklio vidurkis Europoje – 21 proc.). Valstybės tarnautojams Lietuvoje taip pat sudaryta galimybė tobulinti įgūdžius kibernetinio saugumo srityje. Kibernetinio saugumo kursus išklausiusių valstybės tarnautojų skaičius kiekvienais metais didėja (Valstybės tarnybos departamento duomenimis, 2015 m. kursus išklausė 146 valstybės tarnautojai, 2016 m. – 249, 2017 m. – 289), bet reguliarūs viešojo ir

[6] IBM. *IBM X-Force Threat Intelligence Index 2018 (2018).*

[7] Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (2018). *2017 m. Nacionalinio kibernetinio saugumo būklės ataskaita*.

privataus sektorių darbuotojų kibernetinio saugumo mokymai, organizuojami atsižvelgiant į naujausias kibernetinio saugumo tendencijas Lietuvoje ir pasaulyje, padidintų darbuotojų atidumą ir kibernetinio saugumo kultūrą.

26. Siekiant kelti Lietuvos gyventojų kibernetinio saugumo kultūrą, turi būti užtikrinta nuolatinė informacijos sklaida, apimanti aktualią informaciją apie naujausius kibernetinius incidentus ir kitus veiksnius, galinčius sukelti grėsmę asmens duomenų saugumui ar tapti nusikalstamų veikų kibernetinėje erdvėje aukomis. 2017 m. specialaus Eurobarometro 464a tyrimo, skirto europiečių požiūriui į kibernetinį saugumą nustatyti, duomenimis, tik 16 proc. interneto vartotojų Lietuvoje mano, kad rizika tapti nusikalstamų veikų kibernetinėje erdvėje aukomis nedidėja (Europos Sąjungos vidurkis – 11 proc.), tačiau šios srities informacijos sklaida turėtų būti didesnė, nes 49 proc. interneto vartotojų Lietuvoje jaučiasi per mažai informuoti apie nusikalstamų veikų kibernetinėje erdvėje riziką (Europos Sąjungos vidurkis – 51 proc.).

27. Pasaulyje atlikta daug tyrimų ir prognozių, jų išvadose konstatuojama esama ir būsima kibernetinio saugumo įgūdžių stoka[8]. Reikiamą kompetenciją gali užtikrinti kokybiškas ir darbo rinkos poreikius atitinkantis švietimas. Šiuo metu Lietuvoje kibernetinio saugumo programas siūlo keturi universitetai, tačiau, remiantis asociacijos „Infobalt“ ir viešosios įstaigos „Investuok Lietuvoje“ 2018 m. atlikto tyrimo „IRT specialistai Lietuvoje: situacija darbo rinkoje ir darbdavių poreikiai“ duomenimis, padėtis neatitinka darbo rinkos poreikių, todėl, siekiant sumažinti didėjantį atotrūkį tarp kibernetinio saugumo specialistų paklausos ir pasiūlos, turi būti plėtojamos ir stiprinamos esamos ir kuriamos naujos studijų programos, skirtos kibernetinio saugumo specialistams rengti.

Siekiant aukštesnės kibernetinio saugumo kultūros, svarbu, kad su kibernetinio saugumo pagrindais būtų supažindinami vaikai pagal ikimokyklinio ugdymo ir (ar) priešmokyklinio ugdymo bendrąją programas ir mokiniai pagal pradinio, pagrindinio ir vidurinio ugdymo programas, nes IRT vis plačiau taikomos užtikrinant ugdymo ir mokymosi procesą.

Įgyvendinant Lietuvos Respublikos Vyriausybės programoje numatytą pedagogų rengimo bei kvalifikacijos tobulinimo sistemos pertvarkymą, taip pat turėtų būti siekiama kelti pedagogų kvalifikaciją kibernetinio saugumo srityje. Skirtingų ugdymo sričių pedagogai, turintys galimybę plėtoti ir gilinti kompetencijas kibernetinio saugumo srityje, gebės sėkmingai ugdyti mokinius ir studentus ir taip prisidės prie žiniomis ir inovacijomis grįstos visuomenės kūrimo, taip pat ir kibernetinio saugumo didinimo.

28. Daugelio kibernetinio saugumo ekspertų nuomone[9], pasaulyje iki 2019 m. bus mažiausiai 1,5 milijono laisvų kibernetinio saugumo specialistų darbo vietų. Asociacijos „Infobalt“ ir viešosios įstaigos „Investuok Lietuvoje“ 2018 m. atlikto tyrimo „IRT specialistai Lietuvoje: situacija darbo rinkoje ir darbdavių poreikiai“ duomenimis, IRT specialistų skaičius Lietuvoje siekia 22,6 tūkst., per ateinančius trejus metus privačiame sektoriuje papildomai reikės apie 13,3 tūkst. įvairių IRT specialistų. Tyrėjai nepateikė duomenų apie kibernetinio saugumo specialistų trūkumą Lietuvoje, tačiau galima daryti prielaidą, kad kibernetinio saugumo specialistai sudaro reikšmingą trūkstamų specialistų dalį. Sprendžiant kibernetinio saugumo specialistų trūkumo problemą, pirmiausia reikėtų nustatyti, kokių kibernetinio saugumo specialistų šalyje trūksta labiausiai, nes, remiantis kitose valstybėse atliktų tyrimų išvadomis[10], skirtingose valstybėse kibernetinio saugumo specialistų poreikis gali būti skirtingas, gali skirtis ir problemos, susijusios su kibernetinio saugumo įgūdžių stoka, be to, specialistų stokojama ne visose kibernetinio saugumo srityse.

29. Sparčiai plečiantis kibernetinei erdvei atsiranda galimybių diegti inovacijas, kurios yra produktyvumo ir ekonomikos augimo variklis: sudaro galimybes kurti naujų ir geresnių darbo vietų, didina socialinį mobilumą ir yra atsakas į globalius socialinius ir saugumo iššūkius.

---

[8] ISACA. *State of Cybersecurity 2018 (2018),* Information Security Community on LinkedIn, (ISC)^2. *Cybersecurity Trends. 2017 Spotlight Report (2017).*

[9] Silensec. *Addressing the Cyber Security Skills Gap (2017).*

[10] Indeed. *Indeed Spotlight: The Global Cybersecurity Skills Gap (2017),* Information Security Community on LinkedIn, (ISC)^2. *Cybersecurity Trends. 2017 Spotlight Report (2017)*

Lietuva palyginti neseniai įstojo į Europos Sąjungą, todėl čia nėra gilių kibernetinio saugumo mokslinių tyrimų ir mokymo tradicijų, – jos sutelktos kitose Europos Sąjungos valstybėse. Lietuva turi daug galimybių geriau pasinaudoti Europos Sąjungos teikiama investicijų į mokslinius tyrimus skatinimo galimybe – bendrąja mokslinių tyrimų ir inovacijų programa „Horizontas 2020“ (2014–2020 m.) – ir taip prisidėti prie skaitmeninės ekonomikos kūrimo ir gynybos politikos stiprinimo nacionaliniu ir Europos Sąjungos lygiu. Valstybės pastangos turi būti orientuotos į įvairias paramos priemones, suteikiančias privataus sektoriaus atstovams daugiau galimybių įsitraukti į tarptautinius tinklus, ieškant potencialių darbuotojų ir partnerių. Tai paskatintų privatų sektorių investuoti į mokslinių tyrimų, eksperimentinės plėtros ir inovacijų sritis, kurti naujus produktus ir paslaugas, taip pat ir kibernetinio saugumo srityje. Inovatyvių kibernetinio saugumo produktų kūrimas suteiktų papildomą postūmį, paskatintų Lietuvos pramonės konkurencingumą ir yra būtinas siekiant atremti šiuolaikinius kibernetinius incidentus. Taip pat svarbu skatinti Lietuvos mokslininkų dalyvavimą rengiant tarptautines bendras mokslines publikacijas kibernetinio saugumo srityje, pritraukti daugiau studentų, tiesiogiai dalyvauti aukšto lygio kibernetinio saugumo srityje moksliniuose tyrimuose ir eksperimentinės plėtros projektuose, plėtoti viešojo ir privataus sektorių bei mokslo ir studijų institucijų bendradarbiavimą, padidinti užsienio doktorantų kibernetinio saugumo srityje skaičių.

30. 2018 m. Europos inovacijų diegimo rezultatų suvestinės duomenimis, Lietuva, palyginti su kitomis Europos Sąjungos valstybėmis narėmis, yra nuosaikioji inovatorė, tačiau padariusi didelę pažangą skatindama inovacijas ir gerindama inovacijų ekosistemą[11]. Europos Sąjungoje privatus sektorius inovacijoms vis dar skiria mažiau lėšų nei jų konkurentai už Europos Sąjungos ribų. Lietuvoje dar neatlikti patikimi kibernetinio saugumo rinkos matavimai, bet pripažįstama, kad ši rinka yra auganti, todėl inovacijos čia padėtų nuosekliai kurti ir stiprinti konkurencingos šalies, kuriančios inovatyvius kibernetinio saugumo produktus ir paslaugas, statusą. Šios sinergijos galima siekti jungiant inovacijų iniciatyvas su bendrąja valstybės politika, siekiant ilgalaikės mokslo, technologijų ir inovacijų plėtros.

31. Lietuvoje sudaryta finansinių paslaugų veiklai palanki reguliacinė ir priežiūros aplinka, skatinanti inovacijas finansų sektoriuje. Remiantis ataskaitos „Lithuania Fintech Report 2017“ duomenimis, 2017 m. Lietuvoje veikė 117 finansinių technologijų (*FinTech*) įmonių. Ši sritis yra viena iš strateginių Lietuvos banko veiklos krypčių, tad jo veikla vienoje perspektyviausių finansinių technologijų inovacijų – blokų grandinės technologijų (*Blockchain*) – srityje veiksmingai prisidės plėtojant finansinių technologijų inovacijas.

32. **Uždaviniai trečiajam Strategijos tikslui pasiekti:**

32.1. *Pirmasis trečiojo tikslo uždavinys* – plėtoti mokslinius tyrimus ir didelę pridėtinę vertę kuriančias veiklas kibernetinio saugumo srityje. Šis uždavinys bus įgyvendinamas sudarant palankias sąlygas kurti naujas, pažangius gebėjimus plėtojančias kibernetinio saugumo iniciatyvas, skatinant kibernetinio saugumo rinkos augimą, kibernetinio saugumo paslaugų eksportą į užsienio rinkas, plėtojant finansinių technologijų kibernetinio saugumo sektorių ir atliekant mokslinius tyrimus.

32.2. *Antrasis trečiojo tikslo uždavinys* – ugdyti kūrybiškumą, pažangius gebėjimus ir rinkos poreikius atitinkančius kibernetinio saugumo įgūdžius ir kvalifikaciją. Šis uždavinys bus įgyvendinamas viešojo ir privataus sektorių atstovams bei mokslo ir studijų institucijoms kuriant kibernetinio saugumo kompetencijų modelį, formuojant kibernetinio saugumo kompetencijų standartus, plėtojant šios srities mokymų, akreditavimo ir sertifikavimo sistemas, orientuotas į darbo rinkos poreikius, pritraukiant ir ugdant talentus, kuriant kibernetinio saugumo mokymų ir testavimo aplinką, mokant naujokus ir sudarant persikvalifikavimo galimybes IRT srityje dirbantiems asmenims, tobulinant asmenų, dirbančių su jautriais duomenimis, kibernetinio saugumo žinias.

[11] Europos Komisija. *2018 m. Europos inovacijų diegimo rezultatų suvestinė (2018).*

32.3. *Trečiasis trečiojo tikslo uždavinys* – skatinti viešojo ir privataus sektorių bei mokslo ir studijų institucijų bendradarbiavimą, kuriant kibernetinio saugumo srities inovacijas. Šis uždavinys bus įgyvendinamas nustatant bendrus viešojo ir privataus sektorių poreikius ir jų svarbą moksliniams kibernetinio saugumo tyrimams, kuriant technines priemones, metodus ar kitus išteklius, ugdant gebėjimus išspręsti kibernetinio saugumo problemas ar vykdyti specifines kibernetinio saugumo užduotis.

KETVIRTASIS SKIRSNIS
VIEŠOJO IR PRIVATAUS SEKTORIŲ BENDRADARBIAVIMAS

33. **Ketvirtasis Strategijos tikslas** – stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą.

34. Šiuolaikinėse valstybėse, kuriose gerai išvystyta plačiajuosčio ryšio infrastruktūra, viešojo sektoriaus atstovai nebegali toliau vieni kovoti su pavojingais ar didelės reikšmės kibernetiniais incidentais, o ypatingos svarbos informacinės infrastruktūros valdytojai – neretai privataus sektoriaus atstovai – patys ne visada gali suvaldyti kibernetinius incidentus, dažnai peržengiančius jų organizacijos ribas. Taigi viešojo ir privataus sektorių bendradarbiavimas tampa būtina sąlyga visapusiškam kibernetiniam saugumui užtikrinti. Viešojo ir privataus sektorių efektyvaus bendradarbiavimo esminė sąlyga – visavertė partnerystė: abipusis pasitikėjimas ir nauda, todėl viešojo ir privataus sektorių bendradarbiavimas turėtų būti į tai orientuotas.

35. Kibernetinio saugumo taryba yra viešojo ir privataus sektorių bendradarbiavimo politiniu lygmeniu pavyzdys. Turi būti siekiama tobulinti Kibernetinio saugumo tarybos veiklą plečiant viešojo ir privataus sektorių bendradarbiavimą, efektyviai naudojantis Kibernetinio saugumo įstatyme nustatytomis Kibernetinio saugumo tarybos teisėmis.

Punkto pakeitimai:
Nr. 390, 2019-04-24, paskelbta TAR 2019-04-26, i. k. 2019-06920

36. Viešojo ir privataus sektorių bendradarbiavimo įgyvendinimui užtikrinti naudojamas Kibernetinio saugumo informacinis tinklas (toliau – tinklas). Vienas iš tinko tikslų yra dalytis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir tinklo narių bendradarbiavimą kibernetinio saugumo srityje. Tinkle būtina įdiegti priemones, užtikrinančias efektyvų ir abipusį pasitikėjimą skatinantį tinklo narių bendravimą.

37. IRT taikomos labai plačiai ir jų nauda XXI amžiuje neabejotina, tačiau IRT paplitimas kelia klausimą, kaip efektyviai reaguoti į aptiktas IRT saugumo spragas. IRT saugumo spragų ieško asmenys, turintys skirtingų tikslų, tačiau, siekiant atsakingumo atskleidžiant IRT saugumo spragas, svarbu sudaryti galimybę saugumo spragą suradusiam ir norinčiam ją ištaisyti asmeniui bendradarbiauti su kibernetinio saugumo subjektais, kurių IRT saugumo spraga buvo atskleista. Kibernetinio saugumo subjektai, nustatę ir viešai paskelbę IRT saugumo spragų atskleidimo tvarką, apsisaugotų nuo kibernetinių incidentų galimos žalos arba ją labai sumažintų. IRT saugumo spragų atskleidimo tvarkos nustatymas ir viešas paskelbimas prisidėtų prie valstybės kibernetinio saugumo užtikrinimo ir sudarytų daugiau viešojo ir privataus sektorių bendradarbiavimo galimybių.

38. **Uždaviniai ketvirtajam Strategijos tikslui pasiekti:**

38.1. *Pirmasis ketvirtojo tikslo uždavinys* – gerinti viešojo ir privataus sektorių bendradarbiavimo koordinavimą. Šis uždavinys bus įgyvendinamas kuriant tvarų viešojo ir privataus sektorių bendradarbiavimo kibernetinio saugumo srityje modelį, nustatant atsakomybę ir pajėgumus stiprinant valstybės kibernetinį saugumą, efektyvinant viešojo ir privataus sektorių atstovų keitimąsi aktualia informacija apie kibernetines grėsmes, įvykusius kibernetinius incidentus, išmoktas pamokas, plėtojant ankstyvojo perspėjimo sistemą, kuriant naujus arba tobulinant esamus komunikacijos metodus ir procesus.

38.2. *Antrasis ketvirtojo tikslo uždavinys* – didinti viešojo bei mažų ir vidutinių privataus sektorių atstovų kibernetinio saugumo brandą. Šis uždavinys bus įgyvendinamas skatinant viešojo bei mažo ir vidutinio privataus sektorių atstovus tikrintis kibernetinio saugumo būklę, taisyti kibernetinio saugumo spragas.

38.3. *Trečiasis ketvirtojo tikslo uždavinys* – kurti atsakingą viešojo ir privataus sektorių IRT saugumo spragų atskleidimo praktiką. Šis uždavinys bus įgyvendinamas inicijuojant atsakingą viešojo ir privataus sektorių IRT spragų atskleidimo praktiką, nustatant šios srities veiklos principus, metodų, techninių gebėjimų ar kitų priemonių taikymo tvarką.

PENKTASIS SKIRSNIS
TARPTAUTINIS BENDRADARBIAVIMAS

39. **Penktasis Strategijos tikslas** – stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą.

40. Lietuvos nacionalinis saugumas ir visuomenės gerovė tiesiogiai priklauso nuo stabilios, laisvai prieinamos ir saugios kibernetinės erdvės. Atsižvelgdama į tarpvalstybinį, sienų nepaisantį kibernetinių grėsmių ir rizikos pobūdį, Lietuva sieks stiprinti nacionalinį kibernetinį saugumą, aktyviai bendradarbiaudama su dvišaliais ir daugiašaliais partneriais ir tikslingai veikdama tarptautiniuose forumuose, skirtuose kibernetinio saugumo bei pasaulinės interneto erdvės valdymo problemoms spręsti.

41. Lietuva siekia tapti aktyvia kibernetinio saugumo ir interneto valdymo klausimus sprendžiančios tarptautinės bendruomenės dalimi, aktyviai bendradarbiauti su partneriais ir sąjungininkais, sudarant tarptautinį sutarimą dėl teisinio kibernetinės erdvės reguliavimo, pagrįsto tarptautinės teisės normų laikymusi, veiklos šioje erdvėje principų ir normų, atviro interneto apsaugos, žmogaus teisių bei laisvių apsaugos kibernetinėje erdvėje. Ypač daug dėmesio Lietuva skirs bendradarbiavimui kibernetinės gynybos srityje su NATO, Europos Sąjungos ir kitomis demokratinių principų besilaikančiomis šalimis. Lietuva pasisako už kuo artimesnį ir darnų NATO ir Europos Sąjungos bendradarbiavimą šioje srityje, siekiant išvengti funkcijų ir veiklų dubliavimosi. Lietuva stiprins dvišalį politinio ir techninio lygmens bendradarbiavimą, ypač su Jungtinėmis Amerikos Valstijomis.

42. **Uždaviniai penktajam Strategijos tikslui pasiekti:**

42.1. *Pirmasis penktojo tikslo uždavinys* – plėtoti tarptautinį, tarpvalstybinį ir Baltijos regiono šalių bendradarbiavimą kibernetinio saugumo srityje. Šis uždavinys bus įgyvendinamas dalyvaujant Europos Sąjungos, NATO, Jungtinių Tautų, Europos saugumo ir bendradarbiavimo organizacijos, Baltijos regiono ir kitų tarptautinių organizacijų veikloje.

42.2. *Antrasis penktojo tikslo uždavinys* – stiprinti tarptautinius kibernetinio saugumo pajėgumus ir gebėjimus. Šis uždavinys bus įgyvendinamas inicijuojant Nuolatinio struktūrizuoto bendradarbiavimo projektą ir jam vadovaujant, siekiant stiprinti Europos Sąjungos valstybių narių, kurių civiliniai ir kariniai pajėgumai atitinka aukštesnius kriterijus ir kurios tarpusavyje yra susaistytos didesniais įsipareigojimais, bendradarbiavimą kibernetinio saugumo ir gynybos srityje.

42.3. *Trečiasis penktojo tikslo uždavinys* – plėsti dialogą su Jungtinėmis Amerikos Valstijomis kibernetinės gynybos srityje, siekti Jungtinių Amerikos Valstijų dalyvavimo Lietuvos kibernetinio saugumo užtikrinimo projektuose. Šis uždavinys bus įgyvendinamas plėtojant dvišalį Lietuvos ir Jungtinių Amerikos Valstijų politinio ir techninio lygmens bendradarbiavimą kibernetinės gynybos ir saugumo srityje, kartu su Jungtinėmis Amerikos Valstijomis vykdant veiklas, stiprinančias mūsų šalies kibernetinę gynybą ir saugumą.

III SKYRIUS
STRATEGIJOS ĮGYVENDINIMAS IR ATSAKOMYBĖ

43. Siekdama įgyvendinti Strategijos tikslus ir uždavinius, Lietuvos Respublikos Vyriausybė tvirtina tarpinstitucinį veiklos planą, kuriame nustatomos Strategijos įgyvendinimo priemonės ir lėšos joms įgyvendinti. Šio plano rengimą koordinuoja Krašto apsaugos ministerija, dalyvaujant NKSC. Įgyvendinant Strategiją, pagal savo kompetenciją dalyvauja ministerijos, kitos valstybės ir (ar) savivaldybių institucijos, įstaigos ir (ar) organizacijos, nurodytos Strategijos tarpinstituciniame veiklos plane (toliau – Strategijos vykdytojai).

44. Nevyriausybinės organizacijos, suinteresuoti viešojo ir privataus sektorių atstovai, Lietuvos mokslo ir studijų institucijos gali prisidėti prie Strategijos vykdymo, jos tikslų ir uždavinių siekimo.

45. Strategija įgyvendinama iš atitinkamų metų Lietuvos Respublikos valstybės biudžeto asignavimų, savivaldybių biudžetų lėšų, Europos Sąjungos ir kitos tarptautinės finansinės paramos lėšų ir kitų teisėtai gautų lėšų. Už reikalingų finansinių išteklių planavimą, vadovaujantis Kibernetinio saugumo įstatyme įtvirtintu subsidiarumo principu, pagal kompetenciją atsako Strategijos vykdytojai.

46. Strategijos tikslų pasiekimas vertinamas pagal Strategijos įgyvendinimo vertinimo kriterijus ir siekiamas jų reikšmes, nurodytus Strategijos priede. Atliekant Strategijos įgyvendinimo stebėseną ir vertinimą taip pat bus naudojami viešai skelbiami Lietuvos statistikos departamento, Eurostato, sociologinių apklausų ir tyrimų duomenys. Strategijos įgyvendinimo rezultatų stebėseną atlieka Krašto apsaugos ministerija, NKSC ir Kibernetinio saugumo taryba.

47. Strategijos vykdytojai, pasibaigus metams, ne vėliau kaip iki kitų metų sausio 15 d. NKSC pateikia informaciją apie Strategijos įgyvendinimo eigą, veiksmingumą ir tai pagrindžiančius duomenis. Kartu su šia informacija gali būti pateikti siūlymai dėl Strategijos ir (arba) jos įgyvendinamųjų dokumentų tikslinimo. NKSC prašymu Strategijos vykdytojai privalo pateikti ir kitą Strategijos įgyvendinimo rezultatų stebėsenai būtiną informaciją. Visi suinteresuoti subjektai gali teikti pasiūlymus dėl Strategijos nuostatų atnaujinimo visą jos įgyvendinimo laikotarpį.

48. Gavęs Strategijos 47 punkte nurodytą informaciją, NKSC ne vėliau kaip iki einamųjų metų vasario 1 d. Krašto apsaugos ministerijai pateikia susistemintus duomenis apie praėjusių metų Strategijos tikslų ir uždavinių įgyvendinimo būklę, gautus pasiūlymus ir problemines sritis, trukdančias įgyvendinti Strategiją.

49. Krašto apsaugos ministerija kasmet iki kovo 1 d. apibendrina gautą praėjusių metų informaciją ir duomenis apie Strategijos įgyvendinimo eigą, veiksmingumą, susistemintus duomenis apie Strategijos metinį įgyvendinimą pristato Kibernetinio saugumo tarybai ir pateikia Vyriausybei. Vyriausybė dėl Strategijos įgyvendinimo kiekvienais metais atsiskaito Lietuvos Respublikos Seimui pateikdama Nacionalinio saugumo būklės ir plėtros metinę ataskaitą.

50. Visa vieša informacija, susijusi su metiniu ir galutiniu Strategijos įgyvendinimo vertinimu, skelbiama NKSC interneto svetainėje.

51. Likus pusei metų iki nustatyto Strategijos įgyvendinimo laikotarpio pabaigos, NKSC parengia ir Krašto apsaugos ministerijai pateikia Strategijos galutinį įgyvendinimo vertinimą, kuris pristatomas Kibernetinio saugumo tarybai ir pateikiamas Vyriausybei.

_____

Nacionalinės kibernetinio saugumo strategijos
priedas

NACIONALINĖS KIBERNETINIO SAUGUMO STRATEGIJOS ĮGYVENDINIMO VERTINIMO KRITERIJAI IR SIEKIAMŲ JŲ REIKŠMIŲ SĄRAŠAS

Eil. Nr.	Vertinimo kriterijaus pavadinimas	Vertinimo kriterijaus reikšmė			Vertinimo kriterijaus pasiekimo stebėseną atliekanti institucija ar įstaiga
		Pradinė žinoma reikšmė 2017 m.	2021 m.	2023 m.	
Nacionalinės kibernetinio saugumo strategijos (toliau – Strategija) **pagrindinis tikslas** yra efektyviai ir laiku identifikuojant kibernetinius incidentus, užkertant kelią jų atsiradimui ir plitimui, valdant kibernetinių incidentų sukeltas pasekmes užtikrinti galimybę Lietuvos visuomenei saugiai naudotis informacinių ir ryšių technologijų teikiamomis galimybėmis					
	Lietuvos Respublikos vieta pasauliniame kibernetinio saugumo indekse, ne mažesnė nei nurodyta	57	30	20	Krašto apsaugos ministerija
1.	Kibernetinių incidentų grėsmės lygis, ne didesnis nei nurodyta	3,4	3,2	3	Krašto apsaugos ministerija
Pirmasis Strategijos tikslas – stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą					
2.	Kibernetinio saugumo reikalavimus atitinkančių kibernetinių saugumo subjektų dalis procentais, ne mažesnė nei nurodyta	*	35	50	Krašto apsaugos ministerija
3.	Viešojo sektoriaus interneto svetainių, į kurias sunku įsilaužti, dalis procentais, ne mažesnė nei nurodyta	25	28	32	Krašto apsaugos ministerija
4.	Nacionalinėse kibernetinio saugumo pratybose dalyvaujančių ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių valdytojų dalis, ne mažesnė nei nurodyta	42	60	70	Krašto apsaugos ministerija
5.	Modernizuoti valstybės kibernetinio saugumo ir kibernetinės gynybos pajėgumai procentais, ne mažiau nei nurodyta	Riboto naudojimo (toliau –	RN	RN	Krašto apsaugos ministerija

Eil. Nr.	Vertinimo kriterijaus pavadinimas	Vertinimo kriterijaus reikšmė			Vertinimo kriterijaus pasiekimo stebėseną atliekanti institucija ar įstaiga
		Pradinė žinoma reikšmė 2017 m.	2021 m.	2023 m.	
		RN)			
Antrasis Strategijos tikslas – užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą					
6.	Mokymus baigusių pareigūnų, prokurorų, specialistų, ekspertų, dalyvaujančių tiriant nusikalstamas veikas kibernetinėje erdvėje, dalis procentais, ne mažesnė nei nurodyta	*	70	90	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
7.	Sukurtų ar įdiegtų techninių įrankių, procedūrų, analizės platformų, skirtų kovai su nusikalstamomis veikomis kibernetinėje erdvėje, skaičius vienetais, ne mažesnis nei nurodyta	*	2	5	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
8.	Projektų, skirtų nusikalstamų veikų kibernetinėje erdvėje prevencijai ir kontrolei stiprinti, skaičius vienetais, ne mažesnis nei nurodyta	2	2	2	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
9.	Dalyvavimo nusikalstamų veikų kibernetinėje erdvėje prevencijos ir tyrimo tarptautiniuose renginiuose ir darbo grupėse skaičius vienetais, ne mažesnis nei nurodyta	12	14	15	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
10.	Dalyvavimo tarptautinėse operacijose, tiriant nusikalstamas veikas kibernetinėje erdvėje, skaičius vienetais, ne mažesnis nei nurodyta	3	4	6	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
Trečiasis Strategijos tikslas – skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą					
11.	Kibernetinio saugumo srities inovacijų plėtrą skatinančių projektų skaičius, iš viso nuo 2018 m.	0	5	10	Krašto apsaugos ministerija kartu su Strategijos

Eil. Nr.	Vertinimo kriterijaus pavadinimas	Vertinimo kriterijaus reikšmė			Vertinimo kriterijaus pasiekimo stebėseną atliekanti institucija ar įstaiga
		Pradinė žinoma reikšmė 2017 m.	2021 m.	2023 m.	
					vykdytojais
12.	Investicijų į kibernetinio raštingumo kultūros skatinimą, saugumo žinių, mokslinių tyrimų plėtrą, suma tūkstančiais eurų, ne mažesnė nei nurodyta	*	1 000	2 000	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
13.	Asmenų, įgijusių kibernetinio saugumo kvalifikaciją, skaičius vienetais, ne mažesnis nei nurodyta.	33	200	400	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
14.	Per Valstybės tarnautojų registro ir valstybės tarnybos valdymo informacinės sistemos modulį mokytų institucijų ir įstaigų valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis, dalis procentais, ne mažesnė nei nurodyta	0	10	70	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
Ketvirtasis Strategijos tikslas – stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą					
15.	Sukurtas viešojo ir privataus sektorių bendradarbiavimo kibernetinio saugumo srityje modelis, vienetais	0	0	1	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
16.	Įtrauktų į kibernetinio saugumo informacinį tinklą valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros valdytojų dalis procentais, ne mažesnė nei nurodyta	36	86	90	Krašto apsaugos ministerija
17.	Priemonių, skirtų viešojo bei mažų ir vidutinių privataus sektorių atstovų kibernetinio saugumo būklei gerinti, skaičius vienetais, ne mažesnis nei nurodyta	0	4	6	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
18.	Priemonių, skirtų atsakingai viešojo ir privataus sektorių IRT saugumo spragų atskleidimo praktikai formuoti, skaičius vienetais,	0	1	2	Krašto apsaugos ministerija kartu su

Eil. Nr.	Vertinimo kriterijaus pavadinimas	Vertinimo kriterijaus reikšmė			Vertinimo kriterijaus pasiekimo stebėseną atliekanti institucija ar įstaiga
		Pradinė žinoma reikšmė 2017 m.	2021 m.	2023 m.	
	ne mažesnis nei nurodyta				Strategijos vykdytojais
Penktasis Strategijos tikslas – stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą					
19.	Dalyvavimo Europos Sąjungos, NATO, Baltijos regiono organizuojamuose susitikimuose, forumuose ar kituose renginiuose kibernetinio saugumo tema, į kuriuos buvo kviečiama, dalis procentais, ne mažesnė nei nurodyta	25	50	70	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
20.	Dalyvavimo tarptautinėse kibernetinių incidentų tyrimo organizacijų darbo grupių susitikimuose, į kuriuos buvo kviečiama, dalis procentais, ne mažesnė nei nurodyta	70	85	100	Krašto apsaugos ministerija
21.	Pasirašytų bendradarbiavimo susitarimų su tarptautinėmis organizacijomis, Europos Sąjungos, NATO, Baltijos regiono ir kitomis šalimis kibernetinio saugumo srityje skaičius vienetais, ne mažesnis nei nurodyta	2	1	2	Krašto apsaugos ministerija kartu su Strategijos vykdytojais

* Pradinė atitinkamo Strategijos įgyvendinimo vertinimo kriterijaus reikšmė nežinoma, nes institucijos, koordinuojančios tam tikro vertinimo kriterijaus atitiktį, neturi duomenų apie šių vertinimo kriterijų reikšmes. Duomenys apie vertinimo kriterijaus reikšmę bus renkami 2019 m.

_____

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2018 m. rugpjūčio 13 d. nutarimu Nr. 818

YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS IDENTIFIKAVIMO METODIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Ypatingos svarbos informacinės infrastruktūros identifikavimo metodikoje (toliau – Metodika) aprašomi ypatingos svarbos informacinės infrastruktūros nustatymo kriterijai ir ypatingos svarbos informacinės infrastruktūros nustatymo procesas.

2. Metodikoje vartojamos sąvokos:

2.1. **Aukščiausio lygio domenų vardų registro tvarkytojas** – subjektas, registruojantis ir administruojantis interneto domenų vardus su konkrečiu aukščiausio lygio domenu.

2.2. **Domenų vardų sistema** – hierarchiškai suskirstyta vardų suteikimo sistema tinkle, kuris persiunčia domenų vardų užklausas.

2.3. **Domenų vardų sistemos paslaugų teikėjas** – subjektas, teikiantis domenų vardų sistemos paslaugas internetu.

2.4. **Informacinė infrastruktūra** – ryšių ir informacinė sistema ar jos dalis, ryšių ir informacinių sistemų grupė, apdorojanti neįslaptintą informaciją.

2.5. **Infrastruktūros objektas** – institucija, įstaiga, įmonė ar jos struktūrinis padalinys, projektuojamas, statomas ar esamas įrenginys, turtas ar jo dalis, kurių valdytojas yra viešasis arba privatus juridinis asmuo.

2.6. **Interneto duomenų srautų mainų taškas** – tinklo įrenginys, per kurį siekiant palengvinti interneto duomenų srautų mainus sujungiamos daugiau nei dvi nepriklausomos autonominės sistemos. Interneto duomenų srautų mainų taškas sujungia tik autonomines sistemas; jį naudojant nebūtina, kad interneto duomenų srautai, kuriais mainosi autonominių sistemų pora, būtų perduodami per trečią autonominę sistemą; be to, jis nekeičia ir netrikdo tokių srautų.

2.7. **Ypatingos svarbos infrastruktūros objektas** – infrastruktūros objektas, teikiantis ypatingos svarbos paslaugą.

2.8. **Ypatingos svarbos paslauga** – paslauga, kurios neveikimas ar veikimo sutrikimas padarytų didelį neigiamą poveikį nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams.

2.9. **Ryšių ir informacinės sistemos tipas** – ryšių ir informacinė sistema ar jos dalis, ryšių ir informacinių sistemų ar jų dalių grupė, elektroninių ryšių tinklas ar jo dalis, elektroninių ryšių tinklų ar jų dalių grupė, informacinė sistema ar jos dalis, informacinių sistemų ar jų dalių grupė, registras ar jo dalis, registrų ar jų dalių grupė, pramoninių procesų valdymo sistema ar jos dalis, pramoninių procesų valdymo sistemų ar jų dalių grupė ir jų valdymo, naudojimo, apsaugos ir priežiūros tikslais laikoma, tvarkoma, atkuriama arba perduodama elektroninė informacija.

2.10. Kitos Metodikoje vartojamos sąvokos suprantamos taip, kaip apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme ir Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme.

3. Ypatingos svarbos informacinės infrastruktūros nustatymo procesą sudaro:

3.1. Metodikos 1 priede nurodytuose ypatingos svarbos sektoriuose veikiančių ir ypatingos svarbos paslaugas teikiančių ypatingos svarbos infrastruktūros objektų nustatymas;

3.2. ypatingos svarbos informacinės infrastruktūros nustatymas ypatingos svarbos infrastruktūros objektuose;

3.3. ypatingos svarbos informacinės infrastruktūros sąrašo projekto vertinimas ir teikimas tvirtinti.

4. Metodikos 1 priede nurodytos institucijos, kurių veiklos sritys apima šiame priede nurodytus ypatingos svarbos sektorius, subsektorius ir juose teikiamas ypatingos svarbos paslaugas (toliau – Atsakinga institucija), paskiria asmenis, atsakingus už ypatingos svarbos sektoriuose veikiančių ir ypatingos svarbos paslaugas teikiančių ypatingos svarbos infrastruktūros objektų ir ypatingos svarbos informacinės infrastruktūros nustatymą, ir pateikia paskirtų atsakingų asmenų kontaktinę informaciją Lietuvos Respublikos krašto apsaugos ministerijai.

5. Pasikeitus atsakingiems asmenims ar kontaktinei informacijai, atnaujinta informacija ne vėliau kaip per penkias darbo dienas nuo įvykusių pasikeitimų dienos pateikiama Krašto apsaugos ministerijai.

II SKYRIUS
YPATINGOS SVARBOS INFRASTRUKTŪROS OBJEKTŲ NUSTATYMAS

6. Ypatingos svarbos infrastruktūros objektai nustatomi šia tvarka:

6.1. Atsakinga institucija nustato visus jos veiklos srityje veikiančius infrastruktūros objektus, turinčius reikšmės teikiant ypatingos svarbos paslaugas, ir kreipiasi į instituciją, įstaigą, įmonę ar jos struktūrinį padalinį, kurie yra infrastruktūros objektai, ar į infrastruktūros objekto valdytoją, kai infrastruktūros objektas yra įrenginys ar įrenginio dalis (toliau – Atsakingas valdytojas), prašydama Atsakingo valdytojo atlikti visų jo valdomų infrastruktūros objektų svarbos vertinimą ir užpildyti Metodikos 2 priede pateiktą klausimyną (toliau – Klausimynas).

6.2. Atsakingas valdytojas ne vėliau kaip per dvidešimt darbo dienų nuo 6.1 papunktyje nurodyto prašymo gavimo dienos užpildo Klausimyną ir teikia jį raštu Atsakingai institucijai. Jeigu Atsakinga institucija ir Atsakingas valdytojas yra tas pats subjektas, Klausimyną pildo Atsakinga institucija.

6.3. Atsakinga institucija įvertina Atsakingo valdytojo pateiktą Klausimyną ir prireikus teikia Atsakingam valdytojui pastabas ir pasiūlymus, kartu nurodydama terminą Klausimynui patikslinti. Atsakinga institucija turi teisę prašyti Atsakingo valdytojo papildomos informacijos, kuri reikalinga Klausimynui patikslinti, taip pat turi teisę Klausimyne papildomai nustatyti ir įvertinti jos veiklos srities sektoriaus specifinius kriterijus, galinčius turėti įtakos jos veiklos srityje veikiančių Atsakingų valdytojų veiklai.

6.4. Infrastruktūros objektų, kurių suminis svarbos balas, atsižvelgiant į Atsakingos institucijos vertinimą, atliktą vadovaujantis Metodikos 15 punkte nurodyta metodine medžiaga, ir Klausimyno kriterijus, sudaro šešiolika ar daugiau balų, teikiamų paslaugų sutrikdymo neigiamas poveikis yra didelis, todėl šie infrastruktūros objektai Atsakingos institucijos nustatomi kaip ypatingos svarbos infrastruktūros objektai.

7. Jeigu ypatingos svarbos infrastruktūros objektus vertinti pradėjusi Atsakinga institucija mano, kad šių objektų nustatymas priskirtinas kitos Atsakingos institucijos kompetencijai, ji kreipiasi į Krašto apsaugos ministeriją, kuri ne vėliau kaip per dvidešimt darbo dienų nuo kreipimosi gavimo dienos priima sprendimą, kuri Atsakinga institucija turi nustatyti ypatingos svarbos infrastruktūros objektus, ir nustato ypatingos svarbos infrastruktūros objektų nustatymo terminą.

III SKYRIUS
YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS NUSTATYMAS

8. Ypatingos svarbos informacinė infrastruktūra nustatoma šia tvarka:

8.1. Atsakinga institucija, Metodikos II skyriuje išdėstyta tvarka nustačiusi ypatingos svarbos infrastruktūros objektus, ne vėliau kaip per dvidešimt darbo dienų nuo užpildyto Klausimyno gavimo dienos kreipiasi į Atsakingą valdytoją prašydama jo nustatyti ypatingos svarbos informacinę infrastruktūrą užpildant Metodikos 3 priede pateiktą ypatingos svarbos informacinės infrastruktūros nustatymo lentelę (toliau – Lentelė) ir įtraukti nustatytą ypatingos svarbos informacinę infrastruktūrą į ypatingos svarbos informacinės infrastruktūros sąrašą (toliau – Sąrašas) užpildant Metodikos 4 priede pateiktą lentelę.

8.2. Atsakingas valdytojas ne vėliau kaip per dvidešimt darbo dienų nuo 8.1 papunktyje nurodyto prašymo gavimo dienos užpildo Lentelę ir Sąrašą ir pateikia juos raštu Atsakingai institucijai. Jeigu Atsakinga institucija ir Atsakingas valdytojas yra tas pats subjektas, Lentelę ir Sąrašą pildo Atsakinga institucija.

8.3. Atsakinga institucija įvertina Atsakingo valdytojo pateiktą Lentelę ir Sąrašą ir prireikus teikia Atsakingam valdytojui pastabas ir pasiūlymus, kartu nurodydama terminą Lentelei ir Sąrašui patikslinti. Atsakinga institucija turi teisę prašyti Atsakingo valdytojo papildomos informacijos, kuri reikalinga Lentelei ir Sąrašui patikslinti.

8.4. Jeigu užpildytame Klausimyne, Lentelėje, Sąraše nurodyta, kad ypatingos svarbos paslauga teikiama dviejose ar daugiau Europos Sąjungos valstybių narių, Atsakinga institucija, prieš priimdama sprendimą dėl ypatingos svarbos informacinės infrastruktūros nustatymo, siekiant nustatyti, kurioje Europos Sąjungos valstybėje turėtų būti taikomas ypatingos svarbos paslaugos reguliavimas, konsultuojasi su Europos Sąjungos valstybių narių institucijomis, kurių veiklos sritys apima užpildytame Klausimyne, Lentelėje, Sąraše nurodytus ypatingos svarbos sektorius, subsektorius ir juose teikiamas ypatingos svarbos paslaugas. Krašto apsaugos ministerija kartu su Nacionaliniu kibernetinio saugumo centru koordinuoja pasikeitimą duomenimis ir informacija, perduodama Europos Sąjungos valstybių narių institucijų, kurių veiklos sritys apima užpildytame Klausimyne, Lentelėje, Sąraše nurodytus ypatingos svarbos sektorius, subsektorius ir juose teikiamas ypatingos svarbos paslaugas.

8.5. Informacinė infrastruktūra, kuri atlikus Atsakingos institucijos vertinimą atitinka visus Lentelėje nurodytus kriterijus, Atsakingos institucijos nustatoma kaip ypatingos svarbos informacinė infrastruktūra.

IV SKYRIUS
NUSTATYTOS YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS SĄRAŠO PROJEKTO VERTINIMAS IR TEIKIMAS TVIRTINTI

9. Ypatingos svarbos informacinė infrastruktūra vertinama šia tvarka:

9.1. Atsakinga institucija, Metodikos III skyriuje nurodyta tvarka nustačiusi ypatingos svarbos informacinę infrastruktūrą, ne vėliau kaip per dvidešimt darbo dienų nuo užpildytos Lentelės ir Sąrašo gavimo remiantis 8.2 papunkčiu dienos (8.4 papunkčio atveju – ne vėliau kaip per penkias darbo dienas nuo konsultacijos su Europos Sąjungos valstybių narių institucijomis pabaigos), užpildo Metodikos 5 priede pateiktą ypatingos svarbos informacinės infrastruktūros, išdėstytos prioriteto tvarka pagal svarbą, sąrašą (toliau – Apibendrintas sąrašas) ir kartu su užpildytu Klausimynu, Lentele ir Sąrašu pateikia Krašto apsaugos ministerijai raštu ir išorinėje kompiuterinėje laikmenoje (CD ar DVD). Apibendrintame sąraše ypatingos svarbos informacinė infrastruktūra surašoma prioriteto pagal svarbą, kuri nustatoma atsižvelgiant į Klausimyne surinktų balų skaičių ir Lentelėje nurodytus kriterijus, tvarka.

9.2. Krašto apsaugos ministerija įvertina Atsakingos institucijos pateiktą Klausimyną, Lentelę, Sąrašą, Apibendrintą sąrašą ir prireikus teikia Atsakingai institucijai pastabas ir pasiūlymus, kartu nurodydama terminą pateiktai informacijai patikslinti. Krašto apsaugos ministerija turi teisę prašyti Atsakingų institucijų papildomos informacijos, reikalingos Klausimynui, Lentelei, Sąrašui ir Apibendrintam sąrašui įvertinti, teikti siūlymus Atsakingai

institucijai įvertinti jos veiklos sričiai priklausančiame ypatingos svarbos sektoriuje paslaugas teikiančius infrastruktūros objektus, kurie nebuvo įtraukti į Apibendrintą sąrašą.

9.3. Krašto apsaugos ministerija ne vėliau kaip per dvidešimt darbo dienų nuo visų Apibendrintų sąrašų gavimo dienos pateikia Nacionaliniam kibernetinio saugumo centrui įvertinti Atsakingų institucijų pateiktus Klausimynus, Lenteles, Sąrašus ir Apibendrintus sąrašus.

9.4. Nacionalinis kibernetinio saugumo centras ne vėliau kaip per trisdešimt darbo dienų nuo 9.3 papunktyje nurodytos informacijos gavimo dienos pateikia Krašto apsaugos ministerijai išvadą dėl Atsakingų institucijų pateiktų Klausimynų, Lentelių, Sąrašų ir Apibendrintų sąrašų atitikties Metodikos reikalavimams ir siūlymus įtraukti ypatingos svarbos informacinę infrastruktūrą ir (arba) šios infrastruktūros valdytojus į sudaromą sąrašą arba jų neįtraukti. Krašto apsaugos ministerija įvertina Nacionalinio kibernetinio saugumo centro pateiktą išvadą ir prireikus teikia Nacionaliniam kibernetinio saugumo centrui pastabas ir pasiūlymus, kartu nurodydama terminą pateiktai išvadai patikslinti.

10. Krašto apsaugos ministerija ne vėliau kaip per trisdešimt darbo dienų nuo 9.4 papunktyje nurodytos išvados gavimo dienos parengia ir teikia Lietuvos Respublikos Vyriausybės nutarimo dėl ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašo tvirtinimo projektą.

11. Atsakingos institucijos ne vėliau kaip per dvidešimt darbo dienų nuo ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašo patvirtinimo dienos informuoja Atsakingus valdytojus apie infrastruktūros objektus ir ypatingos svarbos informacinę infrastruktūrą, kurie įtraukti į Vyriausybės nutarimu patvirtintą ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

12. Atsakingas valdytojas, atsiradus ypatingos svarbos infrastruktūros objekto, ypatingos svarbos informacinės infrastruktūros ir (arba) jos valdymo pokyčių arba kai steigiamas naujas infrastruktūros objektas, skirtas ypatingos svarbos paslaugoms teikti, kurio funkcionavimas pagrįstas informacine infrastruktūra, nedelsdamas, bet ne vėliau kaip per dešimt darbo dienų nuo pokyčių arba sprendimo steigti naują infrastruktūros objektą priėmimo dienos apie tai informuoja Atsakingą instituciją.

13. Atsakinga institucija, gavusi 12 punkte nurodytą informaciją, inicijuoja ypatingos svarbos infrastruktūros objektų peržiūrą ir ne vėliau kaip per dvidešimt darbo dienų nuo 12 punkte nurodytos informacijos gavimo kreipiasi į Atsakingą valdytoją, prašydama atlikti visų jo valdomų infrastruktūros objektų svarbos vertinimą ir užpildyti Klausimyną. Atsakinga institucija nustato ypatingos svarbos infrastruktūros objektus, ypatingos svarbos informacinę infrastruktūrą, ją įvertina ir teikia tvirtinti Metodikos II, III ir IV skyriuose nurodyta tvarka.

14. Jeigu per dvejus metus neįvyksta ypatingos svarbos infrastruktūros objekto, ypatingos svarbos informacinės infrastruktūros ir (arba) jos valdymo pokyčių, Atsakinga institucija inicijuoja ypatingos svarbos infrastruktūros objektų peržiūrą ir ne vėliau kaip per dvidešimt darbo dienų nuo šiame punkte nurodyto dvejų metų termino pabaigos kreipiasi į Atsakingą valdytoją, prašydama jo atlikti visų jo valdomų infrastruktūros objektų svarbos vertinimą ir užpildyti Klausimyną. Atsakinga institucija nustato ypatingos svarbos infrastruktūros objektus, ypatingos svarbos informacinę infrastruktūrą, ją įvertina ir teikia tvirtinti Metodikos II, III ir IV skyriuose nurodyta tvarka.

15. Nacionalinis kibernetinio saugumo centras savo interneto svetainėje skelbia Metodikos prieduose nurodytų Klausimyno, Lentelės, Sąrašo ir Apibendrinto sąrašo automatizuotas pildymo priemones ir metodinę medžiagą.

16. Krašto apsaugos ministerija kas dvejus metus teikia informaciją Europos Komisijai apie nacionalines ypatingos svarbos informacinės infrastruktūros nustatymo priemones, ypatingos svarbos paslaugų sąrašą, Metodikos 1 priede nurodytuose sektoriuose nustatytos informacinės infrastruktūros valdytojų skaičių ir vartotojų skaičiaus nustatymo kriterijus, pasirinktus ypatingos svarbos informacinei infrastruktūrai nustatyti.

_____

Ypatingos svarbos informacinės infrastruktūros
identifikavimo metodikos
1 priedas

YPATINGOS SVARBOS SEKTORIAI, SUBSEKTORIAI, PASLAUGOS IR ATSAKINGOS INSTITUCIJOS

Sektorius	Subsektorius	Paslaugos	Atsakinga institucija
1. Energetikos sektorius	1.1. Elektros energijos subsektorius	1.1.1. Elektros energijos gamybos paslauga	Lietuvos Respublikos energetikos ministerija
		1.1.2. Elektros energijos perdavimo paslauga	
		1.1.3. Elektros energijos skirstymo paslauga	
		1.1.4. Elektros energijos tiekimo paslauga	
	1.2. Naftos ir naftos produktų subsektorius	1.2.1. Naftos gavybos paslauga	
		1.2.2. Naftos perdirbimo ir apdorojimo paslauga	
		1.2.3. Naftos perdavimo vamzdynais paslauga	
		1.2.4. Naftos ir naftos produktų laikymo paslauga (taip pat ir valstybės atsargų saugojimas)	
	1.3. Gamtinių dujų subsektorius	1.3.1. Gamtinių dujų perdavimo paslauga	
		1.3.2. Gamtinių dujų skirstymo paslauga	
		1.3.3. Gamtinių dujų ir suskystintųjų gamtinių dujų laikymo paslauga	
		1.3.4. Gamtinių dujų perdirbimo ir apdorojimo (taip pat ir gamtinių dujų suskystinimo) paslauga	
		1.3.5. Suskystintųjų gamtinių dujų pakartotinio dujinimo paslauga	
		1.3.6. Gamtinių dujų ir suskystintųjų gamtinių dujų tiekimo paslauga	
	1.4. Centralizuoto šildymo subsektorius	1.4.1. Centralizuoto šilumos tiekimo paslauga	
		1.4.2. Centralizuotos šilumos gamybos paslauga	
2. Transporto ir pašto sektorius	2.1. Oro transporto subsektorius	2.1.1. Skrydžių valdymo ir navigacijos paslauga	Lietuvos Respublikos susisiekimo ministerija
		2.1.2. Oro uostų paslauga	
		2.1.3. Oro susisiekimo paslauga	
	2.2. Geležinkelių transporto subsektorius	2.2.1. Keleivių ir bagažo vežimo geležinkeliais paslauga	
		2.2.2. Krovinių vežimo geležinkeliais paslauga	
		2.2.3. Geležinkelių infrastruktūros plėtros, valdymo ir priežiūros paslauga	
	2.3. Vandens transporto subsektorius	2.3.1. Uostų paslauga	
		2.3.2. Laivybos saugos, kontrolės ir valdymo paslauga	
		2.3.3. Keleivių ir krovinių vežimo vandens transportu paslauga	
	2.4. Kelių transporto subsektorius	2.4.1. Susisiekimo kelių transportu paslauga	
		2.4.2. Kelių tinklo planavimo, kontrolės ir priežiūros paslauga	
		2.4.3. Intelektinių transporto sistemų paslauga	

Sektorius	Subsektorius	Paslaugos	Atsakinga institucija
	2.5. Pašto subsektorius	2.5.1. Universalioji pašto paslauga	
3. Finansų sektorius	3.1. Kredito įstaigų subsektorius	3.1.1. Kredito įstaigų finansinė paslauga	Lietuvos Respublikos finansų ministerija
	3.2. Finansinių rinkų infrastruktūros subsektorius	3.2.1. Paslauga, susijusi su mokėjimų ir vertybinių popierių atsiskaitymų sistemų veikla	
		3.2.2. Paslauga, susijusi su prekybos vietų ir (ar) reguliuojamos rinkos veikla	
		3.2.3. Centrinių vertybinių popierių depozitoriumų paslauga	
4. Sveikatos priežiūros sektorius	4.1. Sveikatos priežiūros infrastruktūros subsektorius	4.1.1. Skubiosios medicinos pagalbos paslauga	Lietuvos Respublikos sveikatos apsaugos ministerija
		4.1.2. Stacionarinio gydymo paslauga	
		4.1.3. Ambulatorinio gydymo paslauga	
		4.1.4. Vaistinių preparatų, medicinos priemonių (prietaisų), kraujo ir kraujo komponentų tiekimo ir laikymo paslauga	
		4.1.5. Infekcinių ligų atvejų, protrūkių ir (ar) epidemijų kontrolės paslauga	
5. Geriamojo vandens tiekimo, paskirstymo ir tvarkymo sektorius	5.1. Geriamojo vandens subsektorius	5.1.1. Geriamojo vandens laikymo, tiekimo ir kokybės užtikrinimo paslauga	Lietuvos Respublikos aplinkos ministerija
	5.2. Nuotekų subsektorius	5.2.1. Nuotekų surinkimo ir tvarkymo paslauga	
6. Informacinių technologijų ir elektroninių ryšių sektorius	6.1. Skaitmeninės infrastruktūros subsektorius	6.1.1. Interneto duomenų srautų mainų taško (IXP) paslauga	Lietuvos Respublikos ūkio ministerija
		6.1.2. Domenų vardų sistemos (DNS) paslauga	
		6.1.3. Aukščiausio lygio domenų vardų registro (lt. domeno) paslauga	
		6.1.4. Elektroninės atpažinties paslauga	Lietuvos Respublikos vidaus reikalų ministerija
	6.2. Elektroninių ryšių subsektorius	6.2.1. Fiksuotojo ir judriojo telefono ryšio, duomenų perdavimo paslauga	Lietuvos Respublikos susisiekimo ministerija
		6.2.2. Interneto prieigos paslauga	
		6.2.3. Radijo ir televizijos programų perdavimo ir transliavimo (retransliavimo) paslauga	
	6.3. Informacinių technologijų subsektorius	6.3.1. Duomenų centrų ir (arba) debesijos paslauga	Lietuvos Respublikos ūkio ministerija
7. Aplinkos sektorius	7.1. Oro taršos ir meteorologinio stebėjimo subsektorius	7.1.1. Oro taršos stebėjimo ir ankstyvo perspėjimo paslauga	Lietuvos Respublikos aplinkos ministerija
		7.1.2. Meteorologinio stebėjimo ir ankstyvo perspėjimo paslauga	
	7.2. Paviršinių ir jūros vandenų stebėjimo subsektorius	7.2.1. Paviršinių vandenų (upių, ežerų) stebėjimo ir ankstyvo perspėjimo paslauga	
		7.2.2. Jūros užterštumo stebėjimo ir kontrolės paslauga	
		7.2.3. Vandens lygio reguliavimo, hidrotechninių įrenginių eksploatavimo paslauga	
	7.3. Miškininkystės subsektorius	7.3.1. Valstybinių miškų valdymo paslauga	
8. Civilinės saugos sektorius	8.1. Ekstremaliųjų situacijų valdymo subsektorius	8.1.1. Bendrojo pagalbos centro paslauga	Lietuvos Respublikos vidaus reikalų ministerija
		8.1.2. Perspėjimo apie ekstremaliuosius įvykius ir situacijas, jų likvidavimo, padarinių	

Sektorius	Subsektorius	Paslaugos	Atsakinga institucija
		šalinimo, gyventojų ir turto gelbėjimo organizavimo ir koordinavimo paslauga	
9. Krašto apsaugos sektorius	9.1. Valstybės gynybos subsektorius	9.1.1. Valstybės ginkluotos gynybos paslauga	Lietuvos Respublikos krašto apsaugos ministerija
10. Maisto produktų sektorius	10.1. Maisto produktų tiekimo ir paskirstymo subsektorius	10.1.1. Žemės ūkio ir (ar) maisto produktų gamybos paslauga	Lietuvos Respublikos žemės ūkio ministerija
		10.1.2. Aprūpinimo maistu (valstybės atsargų saugojimo) paslauga	
		10.1.3. Maisto kokybės ir saugos užtikrinimo paslauga	
11. Pramonės sektorius	11.1. Cheminės, branduolinės ir kitos didesnės rizikos pramonės subsektorius	11.1.1. Pavojingų medžiagų gamybos, laikymo ir atliekų tvarkymo paslauga	Lietuvos Respublikos ūkio ministerija Lietuvos Respublikos aplinkos ministerija Lietuvos Respublikos energetikos ministerija
		11.1.2. Didelės rizikos pramoninių objektų saugumo užtikrinimo paslauga	
		11.1.3. Statinių ir kitų objektų sprogdinimo paslauga	
	11.2. Karinės pramonės subsektorius	11.2.1. Karinės įrangos, ginklų ir šaudmenų gamybos paslauga	
12. Užsienio reikalų ir saugumo politikos sektorius	12.1. Užsienio reikalų ir saugumo politikos įgyvendinimo subsektorius	12.1.1. Užsienio reikalų ir saugumo politikos įgyvendinimo paslauga	Lietuvos Respublikos užsienio reikalų ministerija
13. Valstybės valdymo sektorius	13.1. Valstybės valdžios funkcijų vykdymo subsektorius	13.1.1. Valstybės valdžios funkcijų vykdymo paslauga	Lietuvos Respublikos Vyriausybė
		13.1.2. Ypatingos svarbos valstybės informacinių išteklių valdymo ar tvarkymo paslauga	Lietuvos Respublikos ūkio ministerija
14. Viešojo saugumo ir teisinės tvarkos sektorius	14.1. Viešojo saugumo ir teisinės tvarkos užtikrinimo subsektorius	14.1.1. Viešojo saugumo paslauga	Lietuvos Respublikos vidaus reikalų ministerija
		14.1.2. Teisminės ir baudžiamosios sistemos veikimo paslauga	Lietuvos Respublikos teisingumo ministerija

Ypatingos svarbos informacinės infrastruktūros
identifikavimo metodikos
2 priedas

INFRASTRUKTŪROS OBJEKTŲ, UŽTIKRINANČIŲ YPATINGOS SVARBOS PASLAUGŲ TEIKIMĄ, VERTINIMO KLAUSIMYNAS

Atsakinga institucija	
Ypatingos svarbos sektorius	
Ypatingos svarbos subsektorius	
Ypatingos svarbos paslauga	
Ypatingos svarbos paslauga teikiama dviejose ar daugiau Europos Sąjungos valstybių narių	
Ypatingos svarbos infrastruktūros objekto (toliau – objektas) valdytojas	
Objekto pavadinimas	
Pildymo data, versija	
Komentaras	

Eil. Nr.	Klausimas	Koeficientas	A atsakymas	B atsakymas	C atsakymas	D atsakymas	Balas
1.	Sektoriniai klausimai: ar objekto sunaikinimas, sugadinimas ar sutrikdymas padarytų neigiamą poveikį ypatingos svarbos paslaugos teikimui:		3	2	1	0	
1.1.	Elektros energijos subsektoriaus teikiamos paslaugos	3	Elektros energijos tiekimas nutrūktų daugiau nei 145 000 gyventojų arba didesnėje nei 3 savivaldybių teritorijoje, arba I patikimumo kategorijos vartotojui ir tai truktų ilgiau nei 24 valandas	Elektros energijos tiekimas nutrūktų daugiau nei 20 000 gyventojų arba 1/4 savivaldybės teritorijos gyventojų ir tai truktų ilgiau nei 24 valandas	Elektros energijos tiekimas nutrūktų 500 gyventojų ir tai truktų ilgiau nei 24 valandas	Elektros energijos tiekimas nutrūktų mažiau nei 500 gyventojų	
	komentaras						
1.2.	Naftos ir naftos produktų subsektoriaus teikiamos paslaugos	2	Naftos produktų tiekimas sumažėtų daugiau kaip 25 procentais vidutinio dienos suvartojimo	Naftos produktų tiekimas sumažėtų 12–25 procentais vidutinio dienos suvartojimo	Naftos produktų tiekimas sumažėtų 7–12 procentų vidutinio dienos suvartojimo	Naftos produktų tiekimas sumažėtų, bet ne daugiau kaip 7 procentais vidutinio dienos suvartojimo	

Eil. Nr.	Klausimas	Koeficientas	A atsakymas	B atsakymas	C atsakymas	D atsakymas	Balas
						valstybėje	
	komentaras						
1.3.	Gamtinių dujų subsektoriaus teikiamos paslaugos	3	Gamtinių dujų tiekimas nutrūktų daugiau nei 145 000 gyventojų arba didesnėje nei 3 savivaldybių teritorijoje, arba dujų tiekimas būtų nutrauktas vartotojui, kuriam dujos tiekiamos nenutrūkstamai, ir tai truktų ilgiau nei 24 valandas	Gamtinių dujų tiekimas nutrūktų daugiau nei 20 000 gyventojų arba 1/4 savivaldybės teritorijos gyventojų ir tai truktų ilgiau nei 24 valandas	Gamtinių dujų tiekimas nutrūktų daugiau nei 500 gyventojų ir tai truktų ilgiau nei 24 valandas	Gamtinių dujų tiekimas nutrūktų mažiau nei 500 gyventojų	
	komentaras						
1.4.	Centralizuoto šildymo subsektoriaus teikiamos paslaugos	2	Šilumos tiekimas nutrūktų per šildymo sezoną daugiau nei 145 000 gyventojų arba didesnėje nei 3 savivaldybių teritorijoje, arba nenutrūkstamo aprūpinimo šiluma vartotojams ir tai truktų ilgiau nei 24 valandas	Šilumos tiekimas nutrūktų per šildymo sezoną daugiau nei 3 000 gyventojų arba 1/4 savivaldybės teritorijos gyventojų ir tai truktų ilgiau nei 24 valandas	Šilumos tiekimas nutrūktų per šildymo sezoną daugiau nei 500 gyventojų ir tai truktų ilgiau nei 24 valandas	Šilumos tiekimas nutrūktų per šildymo sezoną mažiau nei 500 gyventojų	
	komentaras						
1.5.	Informacinių technologijų ir elektroninių ryšių sektoriaus teikiamos paslaugos	3	Paslaugos teikimas nutrūktų daugiau nei 145 000 gyventojų (viešajame judriojo ar fiksuotojo ryšio tinkle – 37 500 vartotojų arba 1/2 savivaldybės teritorijos) arba didesnei nei 3 savivaldybių teritorijai ir tai truktų ilgiau nei 6 valandas arba ilgiau nei 3 valandoms sutriktų pagalbos skambučių priėmimas	Paslaugos teikimas nutrūktų daugiau nei 100 000 gyventojų (viešajame judriojo ar fiksuotojo ryšio tinkle – 25 000 vartotojų arba 1/3 savivaldybės teritorijos gyventojų) ir tai truktų ilgiau nei 5 valandas arba ilgiau nei valandai sutriktų pagalbos skambučių priėmimas	Paslaugos teikimas nutrūktų daugiau kaip 500 gyventojų ir tai truktų ilgiau nei 24 valandas	Paslaugos teikimas nutrūktų mažiau nei 500 gyventojų	
	komentaras						
1.6.	Geriamojo vandens subsektoriaus	3	Geriamojo vandens tiekimas	Geriamojo vandens	Geriamojo vandens	Geriamojo vandens	

Eil. Nr.	Klausimas	Koeficientas	A atsakymas	B atsakymas	C atsakymas	D atsakymas	Balas
	teikiamos paslaugos		nutrūktų daugiau nei 145 000 gyventojų arba didesnei nei 3 savivaldybių teritorijai ir tai truktų ilgiau nei 24 valandas	tiekimas nutrūktų daugiau kaip 5 000 gyventojų ir tai truktų ilgiau nei 24 valandas arba geriamojo vandens tiekimas nutrūktų stacionarinei asmens sveikatos priežiūros įstaigai, socialinės globos namams, ūkio subjektui ar įstaigai, teikiančiai formaliojo ugdymo paslaugas, ir tai truktų ilgiau nei 24 valandas	tiekimas nutrūktų daugiau kaip 500 gyventojų ir tai truktų ilgiau nei 24 valandas	tiekimas nutrūktų mažiau nei 500 gyventojų	
	komentaras						
1.7.	Nuotekų subsektoriaus teikiamos paslaugos	3	Nuotekų šalinimas sutriktų daugiau nei 145 000 gyventojų arba didesnėje nei 3 savivaldybių teritorijoje ir tai truktų ilgiau nei 24 valandas	Nuotekų šalinimas sutriktų daugiau nei 20 000 gyventojų ir tai truktų ilgiau nei 24 valandas	Nuotekų šalinimas sutriktų daugiau kaip 500 gyventojų ir tai truktų ilgiau nei 24 valandas	Nuotekų šalinimas sutriktų mažiau nei 500 gyventojų	
	komentaras						
1.8.	Oro transporto subsektoriaus teikiamos paslaugos	1	Oro transporto eismas nutrūktų ilgiau nei 12 valandų, jeigu bent viename Lietuvos oro uoste nėra galimybės vežti keleivių ir krovinių oro transportu	Oro transporto eismas nutrūktų ilgiau nei 6 valandoms, jeigu bent viename Lietuvos oro uoste nėra galimybės vežti keleivių ir krovinių oro transportu	Oro transporto eismas nutrūktų ilgiau nei 3 valandoms	Oro transporto eismas nutrūktų trumpiau nei 3 valandoms	
	komentaras						
1.9.	Kelių transporto subsektoriaus teikiamos paslaugos	1	Kelių transporto priemonių eismas magistraliniuose keliuose nutrūktų ilgiau nei 8 valandoms, jeigu nėra apylankos ar galimybės ją įrengti	Kelių transporto priemonių eismas magistraliniuose keliuose nutrūktų ilgiau nei 4 valandoms, jeigu nėra apylankos ar	Kelių transporto priemonių eismas nutrūktų ilgiau nei 8 valandoms krašto keliuose arba ilgiau nei 48 valandoms	Kelių transporto priemonių eismas nutrūktų trumpiau nei 8 valandoms krašto keliuose arba trumpiau nei 48 valandoms	

Eil. Nr.	Klausimas	Koeficientas	A atsakymas	B atsakymas	C atsakymas	D atsakymas	Balas
				galimybės ją įrengti	rajoniniuose keliuose, jeigu nėra apylankos ar galimybės ją įrengti	rajoniniuose keliuose, jeigu nėra apylankos ar galimybės ją įrengti	
	komentaras						
1.10.	Geležinkelių transporto subsektoriaus teikiamos paslaugos	1	Geležinkelių transporto eismas viešojoje geležinkelių infrastruktūroje nutrūktų ilgiau nei 12 valandų, jeigu nėra galimybės vežti keleivių ir krovinių geležinkelių transportu	Geležinkelių transporto eismas nutrūktų ilgiau nei 6 valandoms, jeigu nėra galimybių vežti keleivių ir krovinių geležinkelių transportu	Geležinkelių transporto eismas nutrūktų ilgiau nei 3 valandoms	Geležinkelių transporto eismas nutrūktų trumpiau nei 3 valandoms	
	komentaras						
1.11.	Vandens transporto subsektoriaus teikiamos paslaugos	1	Vandens transporto eismas uoste nutrūktų ilgiau nei 24 valandoms, jeigu nėra galimybės vežti keleivių ir krovinių vandens transportu	Vandens transporto eismas uoste nutrūktų ilgiau nei 12 valandų, jeigu nėra galimybės vežti keleivių ir krovinių vandens transportu	Vandens transporto eismas uoste nutrūktų ilgiau nei 6 valandoms, jeigu nėra galimybės vežti keleivių ir krovinių vandens transportu	Vandens transporto eismas uoste nutrūktų trumpiau nei 6 valandoms	
	komentaras						
1.12.	Pašto subsektoriaus teikiamos paslaugos	1	Paslaugos teikimas nutrūktų daugiau nei 145 000 gyventojų arba didesnei nei 3 savivaldybių teritorijai ir tai truktų ilgiau nei 6 valandas arba ilgiau nei 3 valandoms sutriktų pagalbos skambučių priėmimas	Paslaugos teikimas nutrūktų daugiau nei 100 000 gyventojų ir tai truktų ilgiau nei 5 valandas arba ilgiau nei valandai sutriktų pagalbos skambučių priėmimas	Paslaugos teikimas nutrūktų daugiau kaip 500 gyventojų ir tai truktų ilgiau nei 24 valandas	Paslaugos teikimas nutrūktų mažiau nei 500 gyventojų	
	komentaras						
1.13.	Maisto produktų, sveikatos priežiūros, finansų, viešojo saugumo ir teisinės tvarkos, pramonės, valstybės valdymo, civilinės saugos, aplinkos, užsienio reikalų ir saugumo politikos sektorių	2	Paslaugos teikimas nutrūktų daugiau nei 145 000 gyventojų arba didesnei nei 3 savivaldybių teritorijai ir tai truktų ilgiau nei 24 valandas	Paslaugos teikimas nutrūktų daugiau nei 20 000 gyventojų ir tai truktų ilgiau nei 24 valandas	Paslaugos teikimas nutrūktų daugiau nei 500 gyventojų ir tai truktų ilgiau nei 12 valandų	Paslaugos teikimas nutrūktų trumpiau nei 12 valandų	

Eil. Nr.	Klausimas	Koeficientas	A atsakymas	B atsakymas	C atsakymas	D atsakymas	Balas
	teikiamos paslaugos						
	komentaras						
1.14.	Krašto apsaugos sektoriaus teikiamos paslaugos	Riboto naudojimo (toliau – RN)	RN	RN	RN	RN	
	komentaras						
2.	Ar objekto sunaikinimas, sugadinimas ar sutrikdymas:		3	2	1	0	
2.1.	Sukeltų pavojų gyventojų gyvybei ar sveikatai	1	Pavojus kiltų daugiau nei 87 000 gyventojų gyvybei ar sveikatai arba pavojus gyventojų gyvybei ir sveikatai kiltų didesnėje nei 3 savivaldybių teritorijoje	Pavojus kiltų daugiau nei 1 200 gyventojų gyvybei ar sveikatai	Pavojus kiltų daugiau nei 300 gyventojų gyvybei ar sveikatai	Pavojus kiltų mažiau nei 300 gyventojų gyvybei ir sveikatai	
	komentaras						
2.2.	Padarytų neigiamą poveikį Lietuvos ekonomikai	1	Valstybė prarastų daugiau nei 200 000 produktyvių darbo dienų	Valstybė prarastų daugiau nei 50 000 produktyvių darbo dienų	Valstybė prarastų daugiau nei 10 000 produktyvių darbo dienų	Valstybė prarastų mažiau nei 10 000 produktyvių darbo dienų	
	komentaras						
2.3.	Padarytų žalą aplinkai	1	Būtų padaryta daugiau nei 1 mln. eurų žala aplinkai arba žala žmonių sveikatai	Būtų padaryta daugiau nei 600 tūkst. eurų žala aplinkai	Būtų padaryta daugiau nei 15 tūkst. eurų žala aplinkai	Objekto sunaikinimo, sugadinimo ar sutrikdymo padaryta žala aplinkai būtų mažesnė nei 15 tūkst. eurų arba jos nebūtų	
	komentaras						
2.4.	Padarytų neigiamą poveikį rinkai ar teikiamai paslaugai atsižvelgiant į esamas tos paslaugos teikimo alternatyvas	1	Taip, turėtų esminį poveikį	Taip, turėtų didelį poveikį	Turėtų nedidelį poveikį	Neturėtų poveikio	
	komentaras						
2.5.	Padarytų neigiamą poveikį gyventojų pasitikėjimui savo valstybe	1	Taip, turėtų esminį poveikį	Taip, turėtų didelį poveikį	Turėtų nedidelį poveikį	Neturėtų poveikio	
	komentaras						

Eil. Nr.	Klausimas	Koeficientas	A atsakymas	B atsakymas	C atsakymas	D atsakymas	Balas
2.6.	Padarytų neigiamą poveikį kito objekto, užtikrinančio tos pačios ypatingos svarbos paslaugos teikimą, netrikdomam funkcionavimui	3	Taip (jeigu atsakymas „taip“, nurodyti – kokį)			Ne	
	komentaras						
2.7.	Padarytų neigiamą poveikį kito objekto, užtikrinančio kitų ypatingos svarbos paslaugų teikimą, netrikdomam funkcionavimui	3	Taip (jeigu atsakymas „taip“, nurodyti – kokį)			Ne	
	komentaras						
2.8.	Padarytų neigiamą poveikį viešojo saugumo užtikrinimui	1	Taip, turėtų esminį poveikį	Taip, turėtų didelį poveikį	Turėtų nedidelį poveikį	Neturėtų poveikio	
	komentaras						
2.9.	Padarytų žalą kitoms ES ir (ar) NATO valstybėms narėms	1	Taip, bent dviem ES ir (ar) NATO valstybėms narėms	Taip, vienai ES ir (ar) NATO valstybei narei	ES ir (ar) NATO valstybei narei gali kilti neigiamų padarinių, bet mažai tikėtina, kad jų poveikis būtų didelis	ES ir (ar) NATO valstybės narės žalos nepatirs	
	komentaras						
2.10.	Padarytų neigiamą poveikį valstybės integracijos į europines ir transatlantines institucijas stiprinimui ir tarptautinių saugumo garantijų užsitikrinimui	1	Taip, turėtų esminį poveikį	Taip, turėtų didelį poveikį	Turėtų nedidelį poveikį	Neturėtų poveikio	
	komentaras						
2.11.	Padarytų neigiamą poveikį nacionalinio saugumo interesams	6	Taip, objektas yra priskirtas nacionaliniam saugumui užtikrinti svarbių įmonių kategorijai arba įtrauktas į nacionaliniam saugumui užtikrinti svarbių įrenginių ir turto sąrašą (jeigu atsakymas „taip“, nurodyti – koks)			Ne	
	komentaras						

Eil. Nr.	Klausimas	Koeficientas	A atsakymas	B atsakymas	C atsakymas	D atsakymas	Balas
					Suminis svarbos balas		
					Ar tai ypatingos svarbos infrastruktūros objektas (taip –16 balų ir daugiau / ne – mažiau nei 16 balų)		

Klausimyną užpildė

_____ _____ _____

(pareigų pavadinimas) (parašas) (vardas ir pavardė)

_____

Ypatingos svarbos informacinės infrastruktūros
identifikavimo metodikos
3 priedas

YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS NUSTATYMO LENTELĖ

Atsakinga institucija	
Ypatingos svarbos sektorius	
Ypatingos svarbos subsektorius	
Ypatingos svarbos paslauga	
Ypatingos svarbos paslauga teikiama dviejose ar daugiau Europos Sąjungos valstybių narių	
Ypatingos svarbos infrastruktūros objekto (toliau – objektas) valdytojas	
Objekto pavadinimas	
Suminis svarbos balas	
Pildymo data, versija	
Komentaras	

Informacinės infrastruktūros būtinumo ypatingos svarbos paslaugos netrikdomam teikimui užtikrinti vertinimas:

Eil. Nr.	**Informacinė infrastruktūra**	**Ryšių ir informacinės sistemos tipas**	**Ar informacinė infrastruktūra būtina objekto teikiamai paslaugai užtikrinti (taip / ne)**	**Ar kibernetinis incidentas informacinėje infrastruktūroje gali sutrikdyti objekto teikiamą paslaugą (taip / ne)**	**Ar sutrikus informacinei infrastruktūrai nėra kitų alternatyvų objekto teikiamos paslaugos tęstinumui užtikrinti (taip / ne)**	**Tai ypatingos svarbos informacinė infrastruktūra (jeigu į 3 klausimus atsakyta „taip“) (taip / ne)**	**Pastabos**
1.							
2.							
3.							

Lentelę užpildė

_____ _____ _____

(pareigų pavadinimas) (parašas) (vardas ir pavardė)

_____

Ypatingos svarbos informacinės infrastruktūros
identifikavimo metodikos
4 priedas

YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS SĄRAŠAS

Atsakinga institucija	
Ypatingos svarbos sektorius	
Ypatingos svarbos subsektorius	
Ypatingos svarbos paslauga	
Ypatingos svarbos paslauga teikiama dviejose ar daugiau Europos Sąjungos valstybių narių	
Ypatingos svarbos infrastruktūros objekto (toliau – objektas) valdytojas	
Objekto pavadinimas	
Suminis svarbos balas	
Pildymo data, versija	
Komentaras	

Eil. Nr.	**Ypatingos svarbos informacinė infrastruktūra**	**Ryšių ir informacinės sistemos tipas**	**Ypatingos svarbos informacinės infrastruktūros funkcijos**	**Ypatingos svarbos informacinės infrastruktūros naudotojų skaičius**	**Ypatingos svarbos informacinės infrastruktūros valdytojo kontaktiniai duomenys**	**Pastabos**
1.						
2.						
3.						
4.						
5.						
6.						
7.						

Sąrašą sudarė

_____ _____ _____

(pareigų pavadinimas) (parašas) (vardas ir pavardė)

Ypatingos svarbos informacinės infrastruktūros
identifikavimo metodikos
5 priedas

YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS, IŠDĖSTYTOS PRIORITETO PAGAL SVARBĄ TVARKA, SĄRAŠAS

Eil. Nr.	Atsakinga institucija	Ypatin-gos svarbos sekto-rius	Ypatingos svarbos subsekto-rius	Ypatingos svarbos paslauga	Ypatingos svarbos informacinė infrastruk-tūra	Ryšių ir informacinės sistemos tipas	Ypatingos svarbos informacinės infrastruk-tūros funkcijos	Ypatingos svarbos informacinės infrastruk-tūros valdytojo kontaktiniai duomenys	Ypatingos svarbos infrastruk-tūros objekto pavadinimas	Ypatingos svarbos infrastruk-tūros objekto valdytojas	Sumi-nis svarbos balas	Pas-ta-bos
1.												
2.												
3.												
4.												
5.												
6.												
7.												

Sąrašą sudarė

_____ _____ _____

(pareigų pavadinimas) (parašas) (vardas ir pavardė)

Priedo pakeitimai:
Nr. 390, 2019-04-24, paskelbta TAR 2019-04-26, i. k. 2019-06920

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2018 m. rugpjūčio 5 d. nutarimu Nr. 818

ORGANIZACINIŲ IR TECHNINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ, TAIKOMŲ KIBERNETINIO SAUGUMO SUBJEKTAMS, APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas (toliau – Aprašas) nustato organizacinius ir techninius kibernetinio saugumo reikalavimus (toliau kartu – Reikalavimai) kibernetinio saugumo subjektams.

2. Apraše vartojamos sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme 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“ (toliau – Bendrieji elektroninės informacijos saugos reikalavimai).

II SKYRIUS
KIBERNETINIO SAUGUMO SUBJEKTŲ RYŠIŲ IR INFORMACINIŲ SISTEMŲ RIZIKOS VERTINIMAS

3. Kibernetinio saugumo subjektų ryšių ir informacinių sistemų kibernetinio saugumo organizacinių ir techninių priemonių užtikrinimas grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos ryšių ir informacinių sistemų kibernetiniam saugumui, rizikos vertinimu, atsižvelgiant į naujausius technikos laimėjimus. Kibernetinio saugumo subjektai, organizuodami ryšių ir informacinių sistemų rizikos vertinimą:

3.1. paskiria už rizikos vertinimą, rizikos vertinimo proceso priežiūrą bei nuolatinį tobulinimą atsakingą asmenį arba asmenis ir nustato jiems taikomus kvalifikacinius reikalavimus. Atsakingu asmeniu gali būti skiriamas kibernetinio subjekto darbuotojas arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros bei nuolatinio tobulinimo paslaugas teikiančiu subjektu;

3.2. nustato reikalavimus rizikos vertinimo procesui, rizikos išdėstymo pagal prioritetus kriterijus ir priimtiną rizikos lygį;

3.3. nustato grėsmes ir pažeidžiamumus, galinčius turėti įtakos ryšių ir informacinių sistemų kibernetiniam saugumui, ir nustato galimo grėsmių ir pažeidžiamumų poveikio vykdomai veiklai sritis;

3.4. įvertina ryšių ir informacinių sistemų pažeidimo grėsmių tikimybę ir pasekmes, nustato rizikos lygį, įvertina identifikuotas grėsmių tikimybes ir jas išdėsto prioriteto tvarka pagal svarbą, kuri nustatoma atsižvelgiant į atliktą rizikos vertinimą;

3.5. Aprašo nustatyta tvarka, atsižvelgdami į atliktą rizikos vertinimą, rengia ir (ar) peržiūri patvirtintus teisės aktus, reglamentuojančius valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros kibernetinio saugumo politiką ir jos įgyvendinimą (toliau – kibernetinio saugumo politikos ir jos įgyvendinimo dokumentai),

viešųjų ryšių tinklų ir (arba) viešųjų elektroninių paslaugų kibernetinio saugumo valdymo taisykles, paslaugų kibernetinio saugumo valdymo taisykles, ir nustato, kuriuos iš juose nustatytų kibernetinio saugumo reikalavimų būtina atnaujinti ir (ar) įgyvendinti pirmiausia, siekiant užtikrinti ryšių ir informacinių sistemų kibernetinį saugumą.

4. Organizuojant ryšių ir informacinių sistemų rizikos vertinimą, rekomenduojama vadovautis Lietuvos ir tarptautiniais standartais ar metodikomis, reglamentuojančiais rizikos valdymą, ir įtraukti ryšių ir informacinių sistemų rizikos vertinimą į kibernetinio saugumo subjektų veiklos rizikos vertinimo procesus.

III SKYRIUS
ORGANIZACINIAI KIBERNETINIO SAUGUMO REIKALAVIMAI SUBJEKTAMS, VALDANTIEMS IR (ARBA) TVARKANTIEMS VALSTYBĖS INFORMACINIUS IŠTEKLIUS, YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS VALDYTOJAMS

5. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai:

5.1. ne rečiau kaip kartą per metus arba po esminių organizacinių ar sisteminių pokyčių Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka rizikos vertinimą. Šį rizikos vertinimą subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ir ypatingos svarbos informacinės infrastruktūros valdytojai turi teisę atlikti kartu su valstybės informacinių išteklių rizikos ar ypatingos svarbos informacinės infrastruktūros rizikos ir (arba) informacinių technologijų saugos atitikties vertinimu;

5.2. atsižvelgdami į atlikto rizikos vertinimo rezultatus, taip pat jeigu nustatoma kibernetinių incidentų valdymo ir šalinimo, organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, tobulina valstybės informacinių išteklių veiklos tęstinumo valdymo planus ar kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus. Veiklos tęstinumo valdymo planų ar kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planų veiksmingumo išbandymo rezultatai išdėstomi šių planų veiksmingumo išbandymo ir pastebėtų trūkumų ataskaitose, kurių kopijos ne vėliau kaip per penkias darbo dienas nuo šių dokumentų priėmimo pateikiamos Nacionaliniam kibernetinio saugumo centrui;

5.3. suderinę su Nacionaliniu kibernetinio saugumo centru, tvirtina kibernetinio saugumo politikos ir jos įgyvendinimo dokumentus, kuriuose turi būti nustatyta:

5.3.1. kibernetinio saugumo politikos ir jos įgyvendinimo dokumentų taikymas ir naudojimas;

5.3.2. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų grupių sudarymas, teisių ir prieigos prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros paslaugų ir išteklių suteikimas ir valdymas;

5.3.3. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų pareigos ir funkcijos, susijusios su kibernetiniu saugumu;

5.3.4. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų, kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, mokymai kibernetinio saugumo klausimais;

5.3.5. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų vardų ir slaptažodžių sudarymas, apsauga ir keitimas;

5.3.6. audito įrašų administravimas ir saugojimas;

5.3.7. įsibrovimų aptikimas ir prevencija;

5.3.8. saugus naudojimasis belaidžiu tinklu;

5.3.9. mobiliųjų įrenginių, naudojamų prisijungti prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, saugus naudojimas ir kontrolė;

5.3.10. duomenų, esančių mobiliuosiuose įrenginiuose, šifravimo nuostatos;

5.3.11. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros išteklių naudojimas už organizacijos ribų ir (arba) mobiliaisiais įrenginiais;

5.3.12. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudojamų svetainių saugos valdymas;

5.3.13. grėsmių ir pažeidžiamumų, galinčių turėti įtakos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros kibernetiniam saugumui, vertinimas;

5.3.14. pažeidžiamumų nustatymo dalyvių teisės ir pareigos;

5.3.15. pažeidžiamumų nustatymo plano rengimas;

5.3.16. pažeidžiamumų nustatymo programinės įrangos naudojimas;

5.3.17. pažeidžiamumų nustatymo rezultatų klasifikavimas;

5.3.18. pažeidžiamumų nustatymo ataskaitų rengimas ir nustatytų trūkumų šalinimas;

5.3.19. kibernetinio incidento valdymo organizavimas;

5.3.20. kibernetinio incidento nustatymas;

5.3.21. kibernetinio incidento vertinimas;

5.3.22. kibernetinio incidento stabdymas ir šalinimas;

5.3.23. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros įprastinės veiklos atkūrimas ir maksimalus leistinas paslaugos neveikimo laikas;

5.3.24. įgytos kibernetinių incidentų valdymo patirties vertinimas;

5.3.25. kibernetiniam saugumui užtikrinti naudojamų priemonių diegimo ir šių priemonių parametrų keitimas;

5.3.26. Reikalavimų įgyvendinimo kontrolės ir atitikties vertinimas;

5.3.27. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros kibernetinio saugumo būklės gerinimas;

5.3.28. elektroninio pašto naudojimas.

6. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, Aprašo 5.3 papunkčio nuostatose nurodytą informaciją ar dokumentus turi teisę išdėstyti pagal Bendruosius elektroninės informacijos saugos reikalavimus rengiamuose ir tvirtinamuose saugos dokumentuose. Šiuo atveju paminėti saugos dokumentai derinami Bendruosiuose elektroninės informacijos saugos reikalavimuose nustatyta tvarka.

7. Išvadas, pastabas ir pasiūlymus dėl kibernetinio saugumo politikos ir jos įgyvendinimo dokumentų projektų Nacionalinis kibernetinio saugumo centras turi pateikti per dešimt darbo dienų, jeigu šie projektai didelės apimties (daugiau kaip dešimt puslapių) – per penkiolika darbo dienų, o dėl pakartotinai pateiktų derinti projektų – per penkias darbo dienas nuo jų gavimo. Prieš pateikdamas išvadas, pastabas ir pasiūlymus dėl kibernetinio saugumo politikos ir jos įgyvendinimo dokumentų projektų, Nacionalinis kibernetinio saugumo centras turi teisę paprašyti valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo pateikti kitus valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros saugumą nustatančius dokumentus.

8. Kibernetinio saugumo politikos ir jos įgyvendinimo dokumentai turi būti peržiūrimi (persvarstomi) ne rečiau kaip kartą per metus. Keičiami kibernetinio saugumo politikos ir jos įgyvendinimo dokumentai su Nacionaliniu kibernetinio saugumo centru gali būti nederinami tais atvejais, kai atliekami tik redakciniai pakeitimai. Tokiais atvejais Nacionaliniam kibernetinio saugumo centrui pateikiamos šių dokumentų kopijos.

9. Ne rečiau kaip kartą per metus turi būti organizuojamas ir atliekamas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros atitikties Reikalavimams vertinimas.

10. Ne rečiau kaip kartą per mėnesį turi būti atliekama valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų veiksmų audito įrašų analizė.

11. Ne rečiau kaip kartą per mėnesį turi būti atliekama saugasienių užfiksuotų įvykių analizė ir šalinamos pastebėtos neatitiktys saugumo reikalavimams.

12. Ne rečiau kaip kartą per mėnesį turi būti įvertinami kibernetiniam saugumui užtikrinti naudojamų priemonių programiniai atnaujinimai, klaidų taisymai ir šie atnaujinimai diegiami.

13. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai, pirkdami paslaugas, darbus ar įrangą, susijusius su valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, pirkimo dokumentuose turi iš anksto nustatyti, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas užtikrina atitiktį Reikalavimams.

IV SKYRIUS
TECHNINIAI KIBERNETINIO SAUGUMO REIKALAVIMAI SUBJEKTAMS, VALDANTIEMS IR (ARBA) TVARKANTIEMS VALSTYBĖS INFORMACINIUS IŠTEKLIUS, YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS VALDYTOJAMS

14. Techniniai kibernetinio saugumo reikalavimai subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ir ypatingos svarbos informacinės infrastruktūros valdytojams nustatomi pagal valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros svarbą, kuri išdėstoma taip:

14.1. Ypatingos svarbos informacinė infrastruktūra (YSII);

14.2. pirma kategorija (I);

14.3. antra kategorija (II);

14.4. trečia kategorija (III);

14.5. ketvirta kategorija (IV).

15. Valstybės informacinių išteklių svarbos kategorijos nustatomos vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“.

16. Išsamus techninių kibernetinio saugumo reikalavimų sąrašas pateiktas Aprašo priede.

17. Kibernetinio saugumo priemonės, nurodytos Aprašo priede, turi būti diegiamos atsižvelgiant į naujausius technikos laimėjimus, vadovaujantis gamintojo pateikiama bent viena gerąja saugumo praktikos rekomendacija.

V SKYRIUS
REIKALAVIMAI VIEŠŲJŲ RYŠIŲ TINKLŲ IR (ARBA) VIEŠŲJŲ ELEKTRONINIŲ RYŠIŲ PASLAUGŲ TEIKĖJAMS

18. Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai:

18.1. ne rečiau kaip kartą per dvejus metus arba po esminių organizacinių ar sisteminių pokyčių Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka rizikos vertinimą. Rizikos vertinimą viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai turi teisę atlikti kartu su veiklos rizikos ir (arba) informacinių technologijų saugos atitikties vertinimu;

18.2. įgyvendina organizacines ir technines priemones, užtikrinančias, kad suklastotų interneto protokolo (IP) adresų srautas būtų blokuojamas jų teikiamuose viešuosiuose ryšių tinkluose;

18.3. įgyvendina organizacines ir technines priemones, užtikrinančias, kad elektroninių paslaugų trikdymo atakos srautas būtų blokuojamas jų teikiamuose viešuosiuose ryšių tinkluose;

18.4. įgyvendina organizacines ir technines priemones, užtikrinančias jų viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugoms teikti naudojamų sistemų ir įrangos kibernetinį saugumą;

18.5. tvirtina ir po esminių organizacinių ar sisteminių pokyčių atnaujina savo viešųjų ryšių tinklų ir (arba) viešųjų elektroninių paslaugų kibernetinio saugumo valdymo taisykles, o Nacionalinio kibernetinio saugumo centro reikalavimu, jas pateikia Nacionaliniam kibernetinio saugumo centrui. Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių paslaugų kibernetinio saugumo valdymo taisyklėse nurodoma:

18.5.1. kibernetiniams incidentams valdyti reikalingų priemonių aprašymai;

18.5.2. viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų nepertraukiamo teikimo užtikrinimo planas ir jo taikymo sąlygos bei maksimalus leistinas paslaugos neveikimo laikas;

18.5.3. už kibernetinių incidentų valdymą atsakingų asmenų funkcijos ir atsakomybė;

18.5.4. viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugoms teikti naudojamų sistemų ir įrangos stebėsenos, patikrinimo, testavimo bei auditavimo tvarka ir sąlygos;

18.5.5. atitiktis Lietuvos ir tarptautiniams standartams, apibūdinantiems kibernetinį saugumą ar saugų elektroninės informacijos tvarkymą;

18.6. neatlygintinai informuoja viešųjų elektroninių ryšių paslaugų gavėjus apie priemones, kuriomis viešųjų elektroninių ryšių paslaugų gavėjai gali pasinaudoti kibernetinių incidentų grėsmei, susijusiai su viešųjų elektroninių ryšių paslaugų gavėjų galiniais įrenginiais, pašalinti, ir nurodo tikėtinas tokių priemonių panaudojimo išlaidas;

18.7. ne vėliau kaip prieš penkias darbo dienas informuoja viešųjų elektroninių ryšių paslaugų gavėjus ir Nacionalinį kibernetinio saugumo centrą apie numatomus planinius darbus, kuriuos atliekant yra tikimybė sutrikdyti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų kibernetinį saugumą;

18.8. viešai skelbia rekomendacijas viešųjų elektroninių ryšių paslaugų gavėjams apie priemones kibernetiniam saugumui užtikrinti naudojantis viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų paslaugomis.

VI SKYRIUS
REIKALAVIMAI ELEKTRONINĖS INFORMACIJOS PRIEGLOBOS PASLAUGŲ TEIKĖJAMS IR SKAITMENINIŲ PASLAUGŲ TEIKĖJAMS

19. Elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai:

19.1. ne rečiau kaip kartą per dvejus metus arba po esminių organizacinių ar sisteminių pokyčių Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka rizikos vertinimą. Šį rizikos vertinimą elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai turi teisę atlikti kartu su veiklos rizikos ir (arba) informacinių technologijų saugos atitikties vertinimu;

19.2. kartu su viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjais imasi reikiamų priemonių kibernetiniam saugumui užtikrinti;

19.3. įgyvendina organizacines ir technines priemones, užtikrinančias jų elektroninės informacijos prieglobos ar skaitmeninėms paslaugoms teikti naudojamų sistemų ir įrangos kibernetinį saugumą;

19.4. tvirtina ir po esminių organizacinių ar sisteminių pokyčių atnaujina savo paslaugų kibernetinio saugumo valdymo taisykles, o Nacionalinio kibernetinio saugumo centro reikalavimu jas pateikia Nacionaliniam kibernetinio saugumo centrui. Elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų kibernetinio saugumo valdymo taisyklėse nurodoma:

19.4.1. kibernetiniams incidentams valdyti reikalingų priemonių aprašymai;

19.4.2. elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų nepertraukiamo teikimo užtikrinimo planas ir jo taikymo sąlygos bei maksimalus leistinas paslaugos neveikimo laikas;

19.4.3. už kibernetinių incidentų valdymą atsakingų asmenų funkcijos ir atsakomybė;

19.4.4. viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugoms teikti naudojamų sistemų ir įrangos stebėsenos, patikrinimo, testavimo bei auditavimo tvarka ir sąlygos;

19.4.5. atitiktis Lietuvos ir tarptautiniams standartams, apibūdinantiems kibernetinį saugumą ar saugų elektroninės informacijos tvarkymą;

19.5. neatlygintinai informuoja elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjus apie nustatytus kibernetinius incidentus, susijusius su elektroninės informacijos prieglobos ar skaitmeninėmis paslaugomis, priskirtus prie turinčių didelį poveikį, nustatytą Nacionaliniame kibernetinių incidentų valdymo plane;

19.6. ne vėliau kaip prieš penkias darbo dienas informuoja elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų gavėjus ir Nacionalinį kibernetinio saugumo centrą apie numatomus planinius darbus, kuriuos atliekant yra tikimybė sutrikdyti elektroninės informacijos prieglobos ar skaitmeninių paslaugų kibernetinį saugumą;

19.7. informuoja elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjus, kuriose šalyse gali būti saugoma jų elektroninė informacija, kuri kuriama, tvarkoma ar pateikta saugoti naudojantis elektroninės informacijos prieglobos ar skaitmeninėmis paslaugomis, ir kokiais atvejais tokia informacija perkeliama į kitas šalis;

19.8. nustato elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjų įspėjimo apie elektroninės informacijos prieglobos ar skaitmeninių paslaugų kibernetinio saugumo pažeidimus tvarką ir kokių veiksmų tokiu atveju privalo imtis elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjai ir (ar) teikėjai;

19.9. viešai skelbia rekomendacijas elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjams apie priemones kibernetiniam saugumui užtikrinti naudojantis elektroninės informacijos prieglobos ar skaitmeninėmis paslaugomis.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

20. Kibernetinio saugumo subjektai turi teisę nustatyti ir taikyti papildomus Reikalavimus. Jeigu papildomais Reikalavimais nustatomos techninės ir organizacinės kibernetinio saugumo priemonės yra lygiavertės ir apima Apraše nustatytus Reikalavimus, kibernetinio saugumo subjektai turi teisę taikyti tik papildomus Reikalavimus.

21. Kibernetinio saugumo subjektai, išskyrus skaitmeninių paslaugų teikėjus, teikia Nacionaliniam kibernetinio saugumo centrui techninę informaciją, reikalingą jų valdomų ryšių ir informacinių sistemų kibernetiniam saugumui įvertinti. Informacija teikiama:

21.1. Nacionalinio kibernetinio saugumo centro reikalavimu jo nurodytais formatais ir terminais;

21.2. kibernetinio saugumo subjektų iniciatyva.

22. Nacionalinis kibernetinio saugumo centras kibernetinio saugumo subjektų pateiktą informaciją apie kibernetinio saugumo būklę, įskaitant ir konfidencialią informaciją, turi teisę tvarkyti tik tiek, kiek tai būtina kibernetinio saugumo subjektų valdomų ryšių ir informacinių sistemų kibernetiniam saugumui įvertinti.

23. Diegiant techninės kibernetinio saugumo priemones viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams, elektroninės informacijos prieglobos paslaugų teikėjams ir skaitmeninių paslaugų teikėjams rekomenduojama vadovautis Aprašo priede pateiktu techninių kibernetinio saugumo reikalavimų sąrašu.

_____

Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo
priedas

TECHNINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ, TAIKOMŲ SUBJEKTAMS, VALDANTIEMS IR (ARBA) TVARKANTIEMS VALSTYBĖS INFORMACINIUS IŠTEKLIUS, YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS VALDYTOJAMS, SĄRAŠAS

1 lentelė. Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumas ir kontrolė

Reikalavimas	**Kategorija pagal svarbą**				
	Ypatingos svarbos informacinė infrastruktūra (YSII)		**I**	**II**	**V**
1. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros priežiūrą vykdančio asmens (toliau – administratorius) funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo funkcijoms atlikti	x				
2. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojams negali būti suteikiamos administratoriaus teisės	x				
3. Kiekvienas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas turi būti unikaliai atpažįstamas (asmens kodas negali būti naudojamas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui atpažinti)	x				
4. Viešaisiais elektroninių ryšių tinklais perduodamos informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą, virtualųjį privatų tinklą (angl. *Virtual private network, VPN*)	x				
5. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas ar administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone	x				
6. Administratorių tapatumui patvirtinti turi būti naudojamos dviejų veiksnių tapatumo patvirtinimo priemonės (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x				
7. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo teisė dirbti su konkrečiu valstybės informaciniu ištekliumi ar ypatingos svarbos informacine infrastruktūra turi būti sustabdoma, kai valstybės informacinių išteklių ar ypatingos svarbos informacinės	x				

infrastruktūros naudotojas nesinaudoja valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra ilgiau kaip tris mėnesius (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)					
8. Administratoriaus teisė dirbti su valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra turi būti sustabdoma, kai administratorius nesinaudoja valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra ilgiau kaip du mėnesius (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x				
9. Kai įstatymų nustatytais atvejais valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas ar administratorius nušalinamas nuo darbo (pareigų), neatitinka kituose teisės aktuose nustatytų valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo ar administratoriaus kvalifikacinių reikalavimų, taip pat pasibaigia jo darbo (tarnybos) santykiai, jis praranda patikimumą, jo teisė naudotis valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra turi būti panaikinta nedelsiant	x				
10. Nereikalingos ar nenaudojamos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų ir administratoriaus paskyros turi būti blokuojamos nedelsiant ir ištrinamos praėjus audito duomenų nustatytam saugojimo terminui	x				
11. Baigus darbą arba valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su informacija, kuri tvarkoma valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje, negalėtų susipažinti pašaliniai asmenys: turi būti atsijungiama nuo valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, įjungiama ekrano užsklanda su slaptažodžiu (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x				
12. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje neatliekant jokių veiksmų, darbo stotis turi užsirakinti, kad toliau naudotis valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra būtų galima tik pakartotinai patvirtinus savo tapatybę (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą). Laikas, per kurį valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui neatliekant jokių veiksmų darbo stotis užsirakina, nustatomas kibernetinio saugumo politikos ir jos įgyvendinimo dokumentuose, tačiau negali būti ilgesnis kaip penkiolika minučių. Šis reikalavimas netaikomas, jeigu, atlikus ryšių ir informacinių sistemų rizikos vertinimą, nustatomos kitos nustatytą riziką atitinkančios techninės	x				

kibernetinio saugumo priemonės					
13. Prisijungimo prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros slaptažodžių reikalavimai:					
13.1. Slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių	x				
13.2. Slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir panašiai)	x				
13.3. Draudžiama slaptažodžius atskleisti kitiems asmenims	x				
13.4. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys, patvirtinančios valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo tapatumą, turi drausti išsaugoti slaptažodžius (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x				
13.5. Turi būti nustatytas didžiausias leistinas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo mėginimų įvesti teisingą slaptažodį skaičius (ne daugiau kaip penki kartai) (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą). Iš eilės neteisingai įvedus slaptažodį tiek kartų, kiek nustatyta, valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo paskyra turi užsirakinti ir neleisti valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui patvirtinti tapatybės kibernetinio saugumo politikos ir jos įgyvendinimo dokumentuose nustatytą laiką – ne trumpiau kaip penkiolika minučių (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)					
13.6. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo mėginimų įvesti teisingą slaptažodį skaičius – ne daugiau kaip trys kartai (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą). Iš eilės neteisingai įvedus slaptažodį tiek kartų, kiek nustatyta, valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo paskyra turi užsiblokuoti ir turi būti informuojamas administratorius (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x				
13.7. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu	x				
13.8. Papildomi valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo slaptažodžių reikalavimai:					
13.8.1. Slaptažodis turi būti keičiamas ne rečiau kaip kas tris mėnesius	x				

13.8.2. Slaptažodį turi sudaryti ne mažiau kaip aštuoni simboliai (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x				
13.8.3. Keičiant slaptažodį, valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros neturi leisti sudaryti slaptažodžio iš buvusių šešių paskutinių slaptažodžių (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x				
13.8.4. Pirmąkart jungiantis prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, turi būti reikalaujama, kad valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas pakeistų slaptažodį (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x				
13.9. Papildomi administratorių slaptažodžių reikalavimai:					
13.9.1. Slaptažodis turi būti keičiamas ne rečiau kaip kas du mėnesius	x				
13.9.2. Slaptažodį turi sudaryti ne mažiau kaip dvylika simbolių (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x				
13.9.3. Keičiant slaptažodį, taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių trijų paskutinių slaptažodžių (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x				
14. Turi būti patvirtinti asmenų, kuriems suteiktos administratoriaus teisės prisijungti prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, sąrašai, periodiškai peržiūrimi kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą. Sąrašas turi būti nedelsiant peržiūrėtas, kai įstatymų nustatytais atvejais administratorius nušalinamas nuo darbo (pareigų)	x				
15. Turi būti vykdoma administratorių paskyrų kontrolė:					
15.1. Periodiškai tikrinama, ar nėra nepatvirtintų administratoriaus paskyrų					
15.2. Naudojamos administratorių paskyrų kontrolės priemonės, kurios tikrina administratoriaus paskyras. Apie nepatvirtintas administratoriaus paskyras turi būti pranešama kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą	x				
16. Vykdoma valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų paskyrų kontrolė:					
16.1. Tikrinama, ar nėra nepatvirtintų valstybės informacinių išteklių arba ypatingos svarbos informacinės infrastruktūros naudotojų paskyrų, ir pranešama kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, apie nepatvirtintas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų paskyras	x				
16.2. Naudojamos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų paskyrų kontrolės priemonės, kurios periodiškai tikrina valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų paskyras. Apie nepatvirtintas paskyras turi būti pranešama kompetentingam	x				

asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą					
17. Draudžiama valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti į atitinkančius reikalavimus	x				

2 lentelė. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, jos naudotojų ir administratorių atliekamų veiksmų auditas ir kontrolė

Reikalavimas	SII		I	II	V
18. Auditui atlikti turi būti fiksuojama ši informacija:					
18.1. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros elementų įjungimas / išjungimas ar perkrovimas (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x				
18.2. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų, administratoriaus prisijungimas (ir nesėkmingi bandymai prisijungti) / atsijungimas	x				
18.3. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų / administratorių teisių naudotis sistemos / tinklo ištekliais pakeitimai (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x				
18.4. Audito funkcijos įjungimas / išjungimas	x				
18.5. Audito įrašų trynimas, kūrimas ar keitimas	x				
18.6. Laiko ir (ar) datos pakeitimai	x				
19. Audituojamų įrašų laiko žymos turi būti sinchronizuotos ne mažiau kaip vienos sekundės tikslumu	x				
20. Turi būti naudojami mažiausiai du laiko sinchronizavimo šaltiniai	x				
21. Kiekviename audito duomenų įraše turi būti fiksuojama:					
21.1. Įvykio data ir tikslus laikas	x				
21.2. Įvykio rūšis / pobūdis	x				
21.3. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo / administratoriaus ir (arba) valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros įrenginio, susijusio su įvykiu, duomenys	x				
21.4. Įvykio rezultatas	x				
22. Priemonės, naudojamos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais	x				
23. Valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje fiksuojami įvykiai turi būti saugomi techninėje ar programinėje įrangoje, pritaikytoje audito duomenims saugoti	x				
24. Dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant, bet ne vėliau kaip vieną darbo dieną turi būti informuojamas administratorius ir kompetentingas asmuo ar	x				

padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą					
25. Audito duomenys turi būti saugomi ne trumpiau kaip šešiasdešimt dienų, užtikrinant visas prasmingas jų turinio reikšmes (pavyzdžiui, valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo, su kuriuo nutraukti darbo santykiai ir kuris pašalintas iš sistemos, atpažinties duomenys turi būti išsaugoti visą būtiną audito duomenų saugojimo laiką)	x				
26. Draudžiama audito duomenis trinti, keisti, kol nesibaigęs audito duomenų saugojimo terminas	x				
27. Audito duomenų kopijos turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo	x				
28. Naudojimasis audito duomenimis turi būti kontroliuojamas ir fiksuojamas. Audito duomenys turi būti pasiekiami tik administratoriui ir kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą (peržiūros teisėmis)	x				
29. Audito įrašų duomenys turi būti analizuojami administratoriaus ne rečiau kaip kartą per mėnesį ir apie analizės rezultatus informuojamas kompetentingas asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą	x				

3 lentelė. Įsibrovimų aptikimas ir prevencija

Reikalavimas	**SII**		**I**	**II**	**V**
30. Turi būti įdiegtos ir veikti įsibrovimo aptikimo sistemos, kurios stebėtų valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros įeinantį ir išeinantį duomenų srautą ir vidinį srautą tarp svarbiausių tinklo paslaugų					
31. Įvykus įtartinai veiklai, tai turi būti užfiksuojama audito įrašuose ir kuriamas pranešimas, kurį matytų administratorius					
32. Sukurtas pranešimas turi būti klasifikuojamas pagal užfiksuotą įvykį					
33. Įsilaužimo atakų pėdsakai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per dvidešimt keturias valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per septyniasdešimt dvi valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros veiklai vertinimas (testavimas)					
34. Pagrindinėse tarnybinėse stotyse turi būti įjungtos saugasienės, sukonfigūruotos blokuoti visą įeinantį ir išeinantį, išskyrus su valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros funkcionalumu ir administravimu susijusį duomenų srautą					
35. Įsilaužimo aptikimo konfigūracijos ir kibernetinių incidentų aptikimo taisyklės turi būti saugomos elektronine forma atskirai nuo valstybės informacinių išteklių ar ypatingos svarbos informacinės					

infrastruktūros techninės įrangos (kartu nurodant atitinkamas datas (įgyvendinimo, atnaujinimo ir panašiai), atsakingus asmenis, taikymo periodus ir panašiai)					

4 lentelė. Belaidžio tinklo saugumas ir kontrolė

Reikalavimas	SII		I	II	V
36. Leidžiama naudoti tik su kompetentingu asmeniu ar padaliniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą, suderintus belaidžio tinklo įrenginius, atitinkančius techninius kibernetinio saugumo reikalavimus					
37. Turi būti vykdoma belaidžių įrenginių kontrolė:					
37.1. Tikrinami valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje eksploatuojami belaidžiai įrenginiai, kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, pranešama apie neleistinus ar techninių kibernetinio saugumo reikalavimų neatitinkančius belaidžius įrenginius					
37.2. Naudojamos priemonės, kurios apribotų neleistinus ar saugumo reikalavimų neatitinkančius belaidžius įrenginius arba informuotų kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą					
37.3. Leidžiama naudoti tik su kompetentingu asmeniu ar padaliniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą, suderintus belaidės prieigos taškus					
38. Belaidės prieigos taškai gali būti diegiami tik atskirame potinklyje, kontroliuojamoje zonoje					
39. Prisijungiant prie belaidžio tinklo, turi būti taikomas ryšių ir informacinių sistemų naudotojų tapatumo patvirtinimo EAP (angl. *Extensible Authentication Protocol*) / TLS (angl. *Transport Layer Security*) protokolas					
40. Turi būti uždrausta belaidėje sąsajoje naudoti SNMP (angl. *Simple Network Management Protocol*) protokolą					
41. Turi būti uždrausti visi nebūtini valdymo protokolai					
42. Turi būti išjungti nenaudojami TCP (angl. *Transmission Control Protocol*) / UDP (angl. *User Datagram Protocol*) prievadai					
43. Turi būti uždraustas lygiarangis (angl. *peer to peer*) funkcionalumas, neleidžiantis belaidžiais įrenginiais palaikyti ryšį tarpusavyje					
44. Belaidis ryšys turi būti šifruojamas mažiausiai 128 bitų ilgio raktu					
45. Prieš pradedant šifruoti belaidį ryšį, turi būti pakeisti belaidės prieigos stotelėje standartiniai gamintojo raktai					
46. Kompiuteriuose, mobiliuosiuose įrenginiuose turi būti išjungta belaidė prieiga, jeigu jos nereikia darbo funkcijoms atlikti, išjungtas lygiarangis (angl. *peer to peer*) funkcionalumas, belaidė periferinė prieiga					

5 lentelė. Mobiliųjų įrenginių, naudojamų prisijungti prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, saugumas ir kontrolė

Reikalavimas	SII		I	II	V
47. Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumo ir kontrolės reikalavimai, nurodyti šio priedo 1 lentelėje, taikytini pagal valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros svarbos kategoriją					
48. Leidžiama naudoti tik mobiliuosius įrenginius, atitinkančius valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo nustatytus saugumo reikalavimus					
49. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojas turi turėti teises valdyti mobiliuosius įrenginius ir juose įdiegtą programinę įrangą					
50. Turi būti vykdoma mobiliųjų įrenginių kontrolė:					
50.1. Tikrinami valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje naudojami mobilieji įrenginiai, kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, pranešama apie neleistinus ar saugumo reikalavimų neatitinkančius mobiliuosius įrenginius					
50.2. Naudojamos priemonės, kurios apribotų neleistinus ar saugumo reikalavimų neatitinkančius mobiliuosius įrenginius ar kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, informuotų apie neleistinos mobiliosios įrangos prijungimą prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros					
51. Mobiliuosiuose įrenginiuose privalo būti naudojamos centralizuotai valdomos ir atnaujinamos kenkimo programinės įrangos aptikimo, užkardymo ir stebėjimo priemonės					
52. Turi būti įdiegiamos operacinės sistemos ir kiti naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai					
53. Mobiliuosiuose įrenginiuose turi būti naudojamos vykdomojo kodo (angl. *Executable code*) kontrolės priemonės, apribojančios neleistino vykdomojo kodo naudojimą ar informuojančios administratorių apie neleistino vykdomojo kodo naudojimą					
54. Turi būti parengti mobiliųjų įrenginių operacinių sistemų atvaizdai su saugumo nuostatomis. Atvaizde turi būti nustatyti tik veiklai būtini operacinių sistemų komponentai (administravimo paskyros, paslaugos (angl. *Services*), taikomosios programos, tinklo prievadai, atnaujinimai, sisteminės priemonės). Atvaizdai turi būti reguliariai peržiūrimi ir atnaujinami, iškart atnaujinami nustačius naujų pažeidžiamumų ar atakų					
55. Pagal parengtus atvaizdus į mobiliuosius įrenginius turi būti įdiegiama operacinė sistema su saugumo nuostatomis					
56. Mobilieji įrenginiai, kuriais naršoma internete, turi būti apsaugoti nuo judriųjų programų (angl. *Mobile code*) keliamų grėsmių					
57. Prie mobiliųjų įrenginių draudžiama prijungti jiems nepriklausančius įrenginius					
58. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo sprendimu prie mobiliųjų įrenginių gali būti jungiami kiti įrenginiai. Administratoriaus parengtą, su kompetentingu asmeniu ar padaliniu, atsakingu už kibernetinio saugumo					

organizavimą ir užtikrinimą, suderintą leistinų jungti įrenginių sąrašą tvirtina valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojas					
59. Duomenys, perduodami tarp mobiliojo įrenginio ir valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, turi būti šifruojami taikant virtualaus privataus tinklo (angl. *VPN*) technologiją					
60. Jungiantis prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, turi būti patvirtinamas tapatumas; mobiliajame įrenginyje ar jo taikomojoje programinėje įrangoje turi būti uždrausta išsaugoti slaptažodį					
61. Nešiojamasis prietaisas, gaunantis energiją iš integruoto energijos šaltinio ir turintis galimybę perduoti ir (ar) priimti ir apdoroti elektroninius duomenis, siunčiamus fizine terpe, elektromagnetinėmis bangomis ir šviesa, kuriuo nesinaudojama nustatytą laiką (pavyzdžiui, penkias minutes), turi automatiškai užsirakinti					
62. Mobiliuosiuose įrenginiuose privalo būti įdiegtos priemonės, leisiančios nuotoliniu būdu neatkuriamai ištrinti duomenis					
63. Turi būti užtikrinta kompiuterinių laikmenų apsauga					
64. Turi būti šifruojami duomenys ir mobiliųjų įrenginių laikmenose, ir išorinėse kompiuterinėse laikmenose					

6 lentelė. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudojamos interneto svetainės, pasiekiamos iš viešųjų elektroninių ryšių tinklų, saugumas ir kontrolė

Reikalavimas	**SII**		**I**	**II**	**V**
65. Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumo ir kontrolės reikalavimai, nurodyti šio priedo skyriuje „Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumas ir kontrolė“, taikytini pagal valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros svarbos kategoriją					
66. Papildomi atpažinties, tapatumo patvirtinimo ir naudojimosi kontrolės reikalavimai:					
66.1. Draudžiama slaptažodžius saugoti programiniame kode					
66.2. Svetainės, patvirtinančios nuotolinio prisijungimo tapatumą, turi drausti išsaugoti slaptažodžius					
67. Turi būti įgyvendinti svetainės kriptografijos reikalavimai:					
67.1. Atliekant svetainės administravimo darbus ryšys turi būti šifruojamas naudojant ne trumpesnį kaip 128 bitų raktą					
67.2. Šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų. Sertifikato raktas turi būti ne trumpesnis kaip 2048 bitų					
67.3. Turi būti naudojamas TLS (angl. *Transport Layer Security*) standartas					
67.4. Svetainės kriptografinės funkcijos turi būti įdiegtos tarnybinės stoties, kurioje yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. *Hardware security module*)					
67.5. Visi kriptografiniai moduliai turi gebėti saugiai sutrikti (angl. *fail securely*)					

67.6. Kriptografiniai raktai ir algoritmai turi būti valdomi pagal ryšių ir informacinių sistemų valdytojo reikalavimus					
68. Tarnybinės stoties, kurioje yra svetainė, svetainės saugos parametrai turi būti teigiamai įvertinti naudojant Nacionalinio kibernetinio saugumo centro rekomenduojamą testavimo priemonę					
69. Draudžiama tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai					
70. Turi būti naudojama svetainės saugasienė (angl. *Web Application Firewall*). Įsilaužimo atakų pėdsakai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per dvidešimt keturias valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per septyniasdešimt dvi valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros veiklai vertinimas (testavimas)					
71. Turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų: struktūrizuotų užklausų kalbos įskverbties (angl. *SQL injection*), įterptinių instrukcijų atakų (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), paskirstyto atsisakymo aptarnauti (angl. *DDOS*) ir kitų, priemonės; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP)*) interneto svetainėje www.owasp.org					
72. Turi būti naudojama svetainės naudotojo įvedamų duomenų tikslumo kontrolė (angl. *Validation*)					
73. Tarnybinė stotis, kurioje yra svetainė, neturi rodyti svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį					
74. Svetainės saugumo priemonės turi gebėti uždrausti prieigą prie tarnybinės stoties iš IP adresų, vykdžiusių grėsmingą veiklą (nesankcionuoti mėginimai prisijungti, įterpti SQL intarpus ir panašiai)					
75. Atliekamų veiksmų audito ir kontrolės reikalavimai, nurodyti šio priedo skyriuje „Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, jos naudotojų ir administratorių atliekamų veiksmų auditas ir kontrolė“, taikytini pagal valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros svarbos kategoriją					
76. Tarnybinė stotis, kurioje yra svetainė, turi leisti tik svetainės funkcionalumui užtikrinti reikalingus protokolo (angl. *HTTP*) metodus					
77. Turi būti uždrausta naršyti svetainės aplankuose (angl. *Directory browsing*)					
78. Turi būti įdiegta svetainės turinio nesankcionuoto pakeitimo (angl. *Defacement*) stebėsenos sistema					

7 lentelė. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudojamo interneto saugumas ir kontrolė

Reikalavimas	SII		I	II	V
79.Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojas su interneto paslaugos teikėju (-ais) turi būti sudaręs šias sutartis:					
79.1. Reagavimo į kibernetinius incidentus įprastomis darbo valandomis					
79.2. Reagavimo į kibernetinius incidentus po darbo valandų					
79.3. Nepertraukiamo interneto paslaugos teikimo:					
79.3.1. įprastomis darbo valandomis					
79.3.2. dvidešimt keturias valandas per parą, septynias dienas per savaitę					
79.4. Interneto paslaugos sutrikimų registravimo:					
79.4.1. įprastomis darbo valandomis					
79.4.2. dvidešimt keturias valandas per parą, septynias dienas per savaitę					
79.5. Apsaugos nuo valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros trikdymo taikymo (angl. *Denial of Service, DoS*)					

_____

Priedo pakeitimai:
Nr. 390, 2019-04-24, paskelbta TAR 2019-04-26, i. k. 2019-06920

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2018 m. rugpjūčio 13 d. nutarimu Nr. 818

NACIONALINIS KIBERNETINIŲ INCIDENTŲ VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinis kibernetinių incidentų valdymo planas (toliau – Planas) nustato kibernetinių incidentų kategorijas, informavimo apie kibernetinius incidentus, kibernetinių incidentų tyrimo ir kibernetinių incidentų analizės baigus kibernetinių incidentų tyrimą tvarką, valdant kibernetinius incidentus.

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

3. Už kibernetinių incidentų valdymo organizavimą, stebėseną ir analizę nacionaliniu lygiu atsakingas Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos. Valstybinė duomenų apsaugos inspekcija, Lietuvos policija ir kitos institucijos, kurių funkcijos susijusios su kibernetiniu saugumu pagal Kibernetinio saugumo įstatymu priskirtą kompetenciją, tiria ar dalyvauja valdant kibernetinius incidentus.

4. Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija ir Lietuvos policija (toliau bendrai kibernetinius incidentus valdančios ir (ar) tiriančios institucijos – KIVT institucijos, o atskirai – KIVT institucija) paskiria asmenis, su kuriais būtų galima susisiekti visą parą ir kurie būtų atsakingi už keitimąsi informacija kibernetinio incidento valdymo metu, numato šių asmenų pakeičiamumą. Valstybinė duomenų apsaugos inspekcija ir Lietuvos policija pateikia Nacionaliniam kibernetinio saugumo centrui atsakingų asmenų, su kuriais galima susisiekti visą parą, telefono numerius, elektroninio pašto adresus, kitą kontaktinę informaciją, sudarančią sąlygas visą parą keistis informacija kibernetinio incidento valdymo metu.

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

6. Kibernetinio saugumo subjektai pateikia Nacionaliniam kibernetinio saugumo centrui atsakingų asmenų, su kuriais galima susisiekti visą parą, telefono numerius, elektroninio pašto adresus, kitą kontaktinę informaciją, sudarančią sąlygas visą parą keistis informacija kibernetinio incidento valdymo metu.

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

II SKYRIUS
KIBERNETINIŲ INCIDENTŲ KATEGORIJOS

8. Kibernetinių incidentų kategorijos nustatomos pagal poveikį kibernetinio saugumo subjektų ryšių ir informacinėms sistemoms ir (ar) paslaugų teikimui ir (ar) įtaką ryšių ir informacinių sistemų teikiamų paslaugų gavėjams.

9. Kibernetiniai incidentai skirstomi į keturias kategorijas:

9.1. pavojingi kibernetiniai incidentai;

9.2. didelio poveikio kibernetiniai incidentai;

9.3. vidutinio poveikio kibernetiniai incidentai;

9.4. nereikšmingo poveikio kibernetiniai incidentai.

10. Kriterijai, kuriais vadovaujantis kibernetiniai incidentai priskiriami Plano 9 punkte nustatytoms kategorijoms, nustatyti Plano priede.

11. Kibernetinius incidentus Plano 9.2–9.4 papunkčiuose nustatytoms kategorijoms, atsižvelgdami į Plano priede nustatytus kriterijus, priskiria kibernetinio saugumo subjektai, kurių ryšių ir informacinėse sistemose nustatyti kibernetiniai incidentai. Jeigu nustatytas kibernetinis incidentas ir (ar) jo poveikis atitinka bent vieną iš kriterijų, nurodytų Plano priede, būdingų Plano 9.1 papunktyje nustatytai pavojingo kibernetinio incidento kategorijai, kibernetinio saugumo subjektai kibernetinį incidentą priskiria 9.2 papunktyje nustatytai didelio poveikio kibernetinio incidento kategorijai.

12. Kibernetinius incidentus Plano 9.1 papunktyje nustatytai pavojingo kibernetinio incidento kategorijai turi teisę priskirti tik Nacionalinis kibernetinio saugumo centras, jeigu nustatytas kibernetinis incidentas ir (ar) jo poveikis atitinka bent vieną iš kriterijų, nurodytų Plano priede, būdingų pavojingo incidento kategorijai.

III SKYRIUS
INFORMAVIMAS APIE KIBERNETINIUS INCIDENTUS

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

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

13.2. vidutinio poveikio kibernetinius incidentus – ne vėliau kaip per keturias valandas nuo jų nustatymo;

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

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

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

14.2. trumpas kibernetinio incidento apibūdinimas;

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

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

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

15. Skaitmeninių paslaugų teikėjai Nacionalinį kibernetinio saugumo centrą informuoja tik apie didelio poveikio kibernetinius incidentus ir tik tuo atveju, kai skaitmeninių paslaugų teikėjas gali naudotis informacija, kuri reikalinga incidento poveikiui įvertinti.

16. Ypatingos svarbos informacinės infrastruktūros valdytojai, kurių paslaugų teikimas priklauso nuo skaitmeninių paslaugų teikėjų teikiamų paslaugų, nustatę neigiamą poveikį jų valdomos ypatingos svarbos informacinės infrastruktūros veiklai, kurį lėmė skaitmeninių paslaugų teikėjų ryšių ir informacinėse sistemose įvykę sutrikimai, apie šį neigiamą poveikį nedelsdami, bet ne vėliau kaip per vieną valandą nuo neigiamo poveikio

nustatymo informuoja Nacionalinį kibernetinio saugumo centrą ir skaitmeninių paslaugų teikėjus, kurių ryšių ir informacinėse sistemose įvyko nurodyti sutrikimai.

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

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

19. Atsižvelgdamas į kibernetinio incidento paplitimo mastą, nustatytus kriterijus, kuriais vadovaujantis kibernetinis incidentas priskiriamas Plano 9.2–9.4 papunkčiuose nustatytoms kategorijoms, ar kibernetinio incidento poveikį ryšių ir informacinei sistemai, Nacionalinis kibernetinio saugumo centras, gavęs informaciją apie kibernetinį incidentą, turi teisę:

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

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

20. Nacionalinis kibernetinio saugumo centras, įvertinęs gautą informaciją, patvirtina, patikslina arba savarankiškai priskiria kibernetinio incidento kategoriją, nustatytą Plano 9 punkte, ir ne vėliau kaip per vieną valandą nuo informacijos gavimo arba, jeigu kibernetinio saugumo subjekto prašoma papildomos informacijos, nuo papildomos informacijos gavimo informuoja apie tai pranešėją.

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

IV SKYRIUS
KIBERNETINIŲ INCIDENTŲ TYRIMAS

PIRMASIS SKIRSNIS
DIDELIO, VIDUTINIO IR NEREIKŠMINGO POVEIKIO KIBERNETINIŲ INCIDENTŲ TYRIMAS

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

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

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

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

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

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

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

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

24.3. kibernetinio incidento veikimo trukmė;

24.4. kibernetinio incidento šaltinis;

24.5. kibernetinio incidento požymiai;

24.6. kibernetinio incidento veikimo metodas;

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

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

24.9. kibernetinio incidento būsena (aktyvus, pasyvus);

24.10. priemonės, kuriomis kibernetinis incidentas nustatytas;

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

24.12. tikslus laikas, kada bus teikiama pakartotinė kibernetinio incidento tyrimo ataskaita remiantis Plano 23 punktu.

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

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

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

26.2. vidutinio poveikio kibernetinių incidentų tyrimai pradedami tik atlikus didelio poveikio kibernetinių incidentų tyrimus, bet ne vėliau kaip per tris darbo dienas nuo kibernetinio saugumo subjektų pranešimo apie kibernetinį incidentą gavimo.

27. Nereikšmingo poveikio kibernetinių incidentų stebėseną vykdo Nacionalinis kibernetinio saugumo centras ir kibernetinio saugumo subjektai. Jei nereikšmingo poveikio kibernetiniai incidentai Plane nustatyta tvarka priskiriami didesnės reikšmės kibernetinių incidentų kategorijai, jie tiriami vadovaujantis Plane nustatytais reikalavimais.

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

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

ANTRASIS SKIRSNIS

PAVOJINGŲ KIBERNETINIŲ INCIDENTŲ TYRIMAS

30. Nacionalinis kibernetinio saugumo centras, priskyręs kibernetinį incidentą pavojingo kibernetinio incidento kategorijai, atsižvelgdamas į kibernetinio saugumo situaciją nedelsdamas, bet ne vėliau kaip per vieną valandą nuo informacijos apie pavojingą kibernetinį incidentą gavimo informuoja kitas KIVT institucijas Plano 44.2–44.3 papunkčiuose nustatytais pagrindais ir nurodo kibernetinio saugumo subjektams, kad pavojingas kibernetinis incidentas toliau turi būti tiriamas ir valdomas vadovaujantis kibernetinio saugumo subjekto patvirtintais teisės aktais, arba perima pavojingo kibernetinio incidento tyrimą ir (ar) valdymo organizavimą.

31. Kibernetinio saugumo subjektai, Nacionalinio kibernetinio saugumo centro nurodymu toliau tiriantys ir valdantys pavojingą kibernetinį incidentą, ne rečiau kaip kas keturias valandas teikia Nacionaliniam kibernetinio saugumo centrui atnaujintą informaciją apie pavojingo kibernetinio incidento valdymo būklę, kurią sudaro Plano 24 punkte nurodyta informacija. Nacionalinis kibernetinio saugumo centras, atsižvelgdamas į kibernetinio saugumo subjektų teikiamą informaciją, turi teisę perimti pavojingo kibernetinio incidento tyrimą ir (ar) valdymo organizavimą.

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

32.1. nuolat renka, apdoroja informaciją, susijusią su kibernetiniu incidentu, ir ne rečiau kaip kas keturias valandas ją teikia Nacionaliniam kibernetinio saugumo centrui;

32.2. ne rečiau kaip kas keturias valandas teikia Nacionaliniam kibernetinio saugumo centrui informaciją apie atliktus kibernetinio incidento tyrimo ir (ar) valdymo veiksmus ir jų rezultatus, kurią sudaro Plano 24 punkte nurodyta informacija;

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

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

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

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

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

33.4. turi teisę surengti koordinacinį pasitarimą dėl kibernetinio incidento tyrimo ir (ar) valdymo, kuriame privalo dalyvauti suinteresuotų KIVT institucijų atstovai, kibernetinio saugumo subjektų paskirti kompetentingi asmenys, atsakingi už kibernetinio saugumo organizavimą ir užtikrinimą, ir kiti kibernetinio saugumo subjektų atstovai, kuriems būtina dalyvauti, siekiant suvaldyti kibernetinį incidentą. Nacionalinis kibernetinio saugumo centras turi teisę į koordinacinį pasitarimą pakviesti kitų kompetentingų ekspertų.

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

35. 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.

36. Nacionalinis kibernetinio saugumo centras apie pavojingo kibernetinio incidento tyrimo ir (ar) valdymo veiksmų eigą nedelsdamas, bet ne vėliau kaip per vieną valandą nuo

kibernetinio incidento priskyrimo pavojingo kibernetinio incidento kategorijai, informuoja Vyriausybės, Seimo ir Prezidento kanceliarijų ir Krašto apsaugos ministerijos paskirtus atsakingus asmenis ir ne vėliau kaip per keturias valandas nuo kibernetinio incidento priskyrimo pavojingo kibernetinio incidento kategorijai pateikia jiems apibendrintą pavojingų kibernetinių incidentų tyrimo ataskaitą, kurią sudaro Plano 24 punkte nurodyta informacija.

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

38. Nacionalinis kibernetinio saugumo centras apie pavojingo kibernetinio incidento tyrimą ir (ar) valdymą reguliariai, bet ne rečiau kaip kas keturias valandas informuoja Plano 36 punkte nurodytus informacijos gavėjus, pateikdamas atnaujintą pavojingų kibernetinių incidentų tyrimo ataskaitą, o informaciją apie pavojingo kibernetinio incidento suvaldymą ar pasibaigimą šiems gavėjams ir kibernetinio saugumo subjektui pateikia ne vėliau kaip per vieną valandą suvaldžius pavojingą kibernetinį incidentą ar jam pasibaigus. Pavojingo kibernetinio incidento tyrimas baigiamas ir kibernetinis incidentas laikomas suvaldytu ar pasibaigusiu, kai išnyksta kibernetinio incidento poveikis ryšių ir informacinei sistemai ir (ar) atkuriama įprasta ryšių ir informacinių sistemų veikla, atitinkanti kriterijus, kuriuos kibernetinio saugumo subjektai nustato savo kibernetinio saugumo teisės aktuose.

39. Nacionalinis kibernetinio saugumo centras, nustatęs, kad nepakanka turimų KIVT institucijų ir kibernetinio saugumo subjektų išteklių pavojingam kibernetiniam incidentui ištirti ir (ar) suvaldyti, nedelsdamas, bet ne vėliau kaip per vieną valandą nuo šių aplinkybių nustatymo informuoja Vyriausybės kanceliarijos ir Krašto apsaugos ministerijos paskirtus atsakingus asmenis, taip pat krašto apsaugos ministrą, o šis ne vėliau kaip per dvidešimt keturias valandas priima sprendimą dėl pavojingo kibernetinio incidento tyrimo ir (ar) valdymo priemonių.

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

41. Krašto apsaugos ministras ne vėliau kaip per dvidešimt keturias valandas nuo Plano 40 punkte nurodytos informacijos gavimo teikia Lietuvos Respublikos Vyriausybei nutarimo projektą, kuriuo siūloma kibernetinį incidentą pripažinti kibernetinio saugumo krize.

TREČIASIS SKIRSNIS
TARPINSTITUCINIS BENDRADARBIAVIMAS IR KEITIMASIS INFORMACIJA TIRIANT KIBERNETINIUS INCIDENTUS

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

43. Kibernetinio saugumo subjektai, iš KIVT institucijų, kitų juridinių asmenų ar kitų valstybių arba tarptautinių organizacijų ar institucijų, atliekančių kibernetinio saugumo užtikrinimo funkcijas, gavę informacijos apie galimą kibernetinį incidentą jų tvarkomose ar valdomose ryšių ir informacinėse sistemose, imasi veiksmų, reikalingų kibernetiniam incidentui nustatyti ir patvirtinti. Nenustačius kibernetinio incidento požymių, kibernetinio saugumo subjektai KIVT institucijas apie tai informuoja ne vėliau kaip per keturias valandas nuo pranešimo apie kibernetinį incidentą gavimo.

44. KIVT institucija, gavusi informaciją apie kibernetinį incidentą, nedelsdama, bet ne vėliau kaip per dvidešimt keturias valandas nuo informacijos apie kibernetinį incidentą gavimo informuoja kitas KIVT institucijas:

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

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

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

45. KIVT institucija, pagal kompetenciją tirianti kibernetinį incidentą, nustačiusi papildomos informacijos apie kibernetinį incidentą poreikį, turi teisę kreiptis į kitas KIVT institucijas ar kibernetinius subjektus, kurie papildomą informaciją turi pateikti per KIVT institucijos, pagal kompetenciją tiriančios kibernetinį incidentą, prašyme nurodytą terminą.

46. Kibernetinio saugumo subjektai ir KIVT institucijos šiame Plane nurodytą informaciją, susijusią su kibernetiniais incidentais ir jų valdymu, perduoda per kibernetinio saugumo informacinį tinklą, o jeigu tokios galimybės nėra, kitomis saugiomis informacijos perdavimo priemonėmis.

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

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

KETVIRTASIS SKIRSNIS
TARPTAUTINIS BENDRADARBIAVIMAS IR KEITIMASIS INFORMACIJA TIRIANT KIBERNETINIUS INCIDENTUS

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

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

50.1. užtikrina tarpvalstybinį Lietuvos Respublikos ir kitų Europos Sąjungos valstybių narių institucijų bendradarbiavimą ir bendradarbiavimą su šių valstybių bendradarbiavimo grupėmis, reagavimo į kompiuterinius saugumo incidentus tarnybomis (toliau – CSIRT) ir kitomis institucijomis, kad būtų galima vykdyti efektyvią kibernetinio saugumo priežiūrą ir operatyviai keistis informacija tarp suinteresuotų asmenų;

50.2. informuoja Europos Komisiją apie kibernetinių incidentų valdymo proceso mastą (nurodydamas įvykusių kibernetinių incidentų grupes, poveikį, skaičių, kibernetinius incidentus, galimai turėjusius poveikį kitoms Europos Sąjungos valstybėms, ir kitą aktualią informaciją) ir pagrindinius elementus ir kiekvienais metais bendradarbiavimo grupei pateikia suvestinę ataskaitą apie gautus pranešimus, kurioje, be kita ko, nurodomas pranešimų skaičius ir incidentų, apie kuriuos pranešta, pobūdis, taip pat veiksmai, kurių buvo imtasi;

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

50.4. teikia su kibernetiniu saugumu susijusius išankstinius įspėjimus, perspėjimus ir rekomendacijas suinteresuotiems asmenims.

51. Koordinuodamas tarptautinio ir tarpinstitucinio bendradarbiavimo veiksmus, Nacionalinis kibernetinio saugumo centras kibernetinio saugumo subjektų pateikta informacija, įskaitant konfidencialią informaciją ir komercines paslaptis, turi teisę keistis tik tiek, kiek tai yra būtina tarptautiniam ir tarpinstituciniam bendradarbiavimui koordinuoti, ir užtikrina gautos informacijos apsaugą.

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

V SKYRIUS
KIBERNETINIŲ INCIDENTŲ ANALIZĖ BAIGUS KIBERNETINIŲ INCIDENTŲ TYRIMĄ

53. Kibernetinio saugumo subjektai ir KIVT institucijos po kibernetinio incidento suvaldymo ar pasibaigimo pagal kompetenciją atlieka jo analizę. Dėl kibernetinių incidentų, priskirtų nereikšmingo kibernetinio incidento kategorijai, kibernetinio incidento analizė neatliekama.

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

54.1. ne vėliau kaip per trisdešimt darbo dienų po kibernetinio incidento suvaldymo ar pasibaigimo pateikia kibernetinio incidento analizės rezultatus Nacionaliniam kibernetinio saugumo centrui ir kibernetinio saugumo informaciniame tinkle paskelbia susistemintą ir aktualią neįslaptintą informaciją apie kibernetinio incidento nustatymą ir suvaldymą;

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

54.3. įvertina ryšių ir informacinės sistemos riziką ir atitiktį Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams;

54.4. nustačius teisinio reglamentavimo spragų, pakeičia savo kibernetinio saugumo teisės aktus ir (ar) inicijuoja kitų institucijų priimtų teisės aktų pakeitimus.

55. KIVT institucijos turi teisę reikalauti kibernetinio saugumo subjektų ne vėliau kaip per trisdešimt darbo dienų po kibernetinio incidento suvaldymo ar pasibaigimo pateikti papildomą informaciją, reikalingą kibernetinio incidento analizei atlikti.

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

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

56.2. prireikus inicijuoja ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos plano pakeitimus;

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

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

KRITERIJŲ, KURIAIS VADOVAUJANTIS KIBERNETINIAI INCIDENTAI PRISKIRIAMI KIBERNETINIŲ INCIDENTŲ KATEGORIJOMS, SĄRAŠAS

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 % ~~(galimas paslaugų nutraukimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų
1.	Nepageidaujamų laiškų, klaidinančios ar žeidžiančios informacijos platinimas (angl. *abusive content, spam*)	1.1. Nepageidaujami laiškai ir (ar) klaidinančios, žeidžiančios informacijos platinimas trikdo ryšių ir informacinės sistemos (toliau – RIS) veiklą ir (ar) teikiamas paslaugas	N				V					D					P		
		1.2. Nepageidaujamų laiškų ir (ar) klaidinančios, žeidžiančios informacijos platinimas	N																
2.	Kenkimo programinė įranga (angl. *malicious software / code*) Programinė įranga ar jos dalis, kuri padeda neteisėtai	2.1. Aptikta moderni kenkimo programinė įranga (angl. *advanced persistent threat, APT*)					V					D					P		
		2.2. RIS aktyviai kontroliuojama įsibrovėlių (pavyzdžiui, „galinės					V					D					P		

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)			
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 % [illegible]	visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų
	prisijungti prie RIS, ją užvaldyti ir kontroliuoti, sutrikdyti ar pakeisti jų veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę ja naudotis ir neteisėtai pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims	durys“ (angl. *back door*), kompiuterizuotos darbo vietos ar tarnybinės stotys tampa „Botinklo“ (angl. *Botnet*) infrastruktūros dalimi																		
		2.3. Kenkimo programinė įranga, trikdanti saugumo priemonių darbą					V					D					P			
		2.4. Kenkimo programinė įranga, kurią aptinka saugumo priemonės per reguliarų patikrinimą ir (ar) kurią saugumo priemonės automatiškai blokuoja	N				V													
		2.5. Kenkimo programinė įranga, platinama naudojant socialinės inžinerijos metodus	N				V					D					P			
3.	Informacijos rinkimas (angl. *information gathering*)	3.1. RIS paketų / informacijos perėmimas					V					D					P			

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)			
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	~~Sunkumas (galimybė pasiekti vartotoją)~~ visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų
	Žvalgyba ar kita įtartina veikla (angl. *scanning, sniffing*), manipuliavimas naudotojų emocijomis, psichologija, pastabumo stoka, pasinaudojimas technologiniu neišmanymu (angl. *social engineering*), siekiant stebėti ir rinkti informaciją, atrasti silpnąsias vietas, atlikti grėsmę keliančius veiksmus, apgavystės, siekiant įtikinti naudotoją atskleisti informaciją (angl. *phishing*) arba atlikti norimus veiksmus	3.2. RIS klastojimas, siekiant surinkti prisijungimo ar kitą svarbią informaciją, tiksliniai laiškai, kuriuose, pasinaudojant socialinės inžinerijos principais, siekiama išvilioti prisijungimo ir (ar) kitą svarbią informaciją, priversti atlikti norimus veiksmus (pvz., finansines operacijas)					V					D					P			
		3.3. Vykdoma perimetro priemonių žvalgyba (nebandant įsilaužti)	N				V													
		3.4. Naudojami socialinės inžinerijos metodai, siekiant išvilioti prisijungimo prie RIS ir (ar) kitą svarbią informaciją	N				V													

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)			
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 % šalies (gali skirtis, priklausyti nuo [illegible])	visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų
4.	Mėginimas įsilaužti (angl. *intrusion attempts*) Mėginimas įsilaužti arba sutrikdyti RIS veikimą išnaudojant žinomus pažeidžiamumus (angl. *exploiting of known vulnerabilities*), bandant parinkti slaptažodžius (angl. *login attempts*), kitą įsilaužimo būdą (angl. *new attack signature*)	4.1. Išnaudojamas vienas ar keli nežinomi (angl. *zero day*) pažeidžiamumai, siekiant tikslingai sutrikdyti konkrečią RIS					V					D					P			
		4.2. Išnaudojamas vienas ar keli nežinomi (angl. *zero day*) pažeidžiamumai	N				V					D					P			
		4.3. Vidinė RIS žvalgyba ar kita kenkimo veika (prievadų skenavimas, slaptažodžių parinkimas, kenkimo programinės įrangos platinimas ir kita)					V					D					P			
		4.4. Išnaudojami žinomi ir viešai publikuoti pažeidžiamumai arba atliekami bandymai prisijungti prie RIS parenkant slaptažodžius	N				V													
5.	Įsilaužimas (angl.	5.1. Veiksmai prieš RIS ar jos					V					D					P			

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)			
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 % ~~(galimas paslaugų poveikis visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų*
	intrusions) Sėkmingas įsilaužimas ir (ar) neteisėtas RIS, taikomosios programinės įrangos ar paslaugos naudojimas (angl. *privileged account compromise, unprivileged account compromise, application compromise*)	saugumo priemones, informacijos pasisavinimas, naikinimas, RIS ar jos dalies pažeidimas, sutrikdantis RIS teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomos informacijos ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti RIS naudotojų pasitikėjimą jais																		
		5.2. Gaunama neteisėta prieiga prie RIS, taikomosios programinės įrangos ar paslaugos					V					D					P			
6.	Paslaugų trikdymas, prieinamumo pažeidimai (angl. *availability*) Veiksmai, kuriais trikdoma	6.1. Teikiamų paslaugų nutraukimas arba maksimalaus leistino paslaugos neveikimo laiko viršijimas					V					D					P			

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento pogrupiai / Kibernetinio incidento poveikis	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)			
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 % ~~(galimas paslaugų teikimo visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų*
	RIS veikla, teikiamos paslaugos (angl. *DoS, DDoS*), RIS ar jos dalies pažeidimas, sutrikdantis RIS ir (ar) jos teikiamas paslaugas (angl. *sabotage, outage*)	6.2. Teikiamų paslaugų nepertraukiamo teikimo trikdymas, galintis turėti įtakos tvarkomos informacijos ir (ar) teikiamų paslaugų prieinamumui	N				V													
		6.3. Aptinkamas paslaugos trikdymas, kuris neturi įtakos paslaugų teikimui	N				V													
7.	Informacijos turinio saugumo pažeidimai (angl. *information content security*) Neteisėta prieiga prie informacijos, neteisėtas informacijos keitimas (angl. *unauthorised access to information, unauthorised*	7.1. Neteisėta prieiga prie informacijos, galinčios turėti įtakos RIS veiklai ir (ar) teikiamoms paslaugoms					V					D					P			
		7.2. Neteisėta prieiga prie informacijos, neteisėtas informacijos keitimas	N				V					D					P			

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)			
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 % ~~šalies teritorijoje, paslaugų teikimas~~ visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų
	modification of information)																			
8.	Neteisėta veikla, sukčiavimas (angl. *fraud*) Vagystė, apgavystė, neteisėtas išteklių (angl. *unauthorized use of resources*), nelegalios programinės įrangos ar autorių teisių (angl. *copyright*) naudojimas, tapatybės klastojimo, apgavystės ir kiti panašaus pobūdžio incidentai	8.1. Neteisėta įtaka RIS veiklai ir (ar) teikiamoms paslaugoms	N				V					D					P			
9.	Kita Incidentai, kurie neatitinka nė vienos iš nurodytų grupių aprašymų		N				V					D					P			

Priedo pakeitimai:

Nr. 390, 2019-04-24, paskelbta TAR 2019-04-26, i. k. 2019-06920

Pakeitimai:

1.
Lietuvos Respublikos Vyriausybė, Nutarimas
Nr. 1209, 2018-12-05, paskelbta TAR 2018-12-10, i. k. 2018-20153
Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo

2.
Lietuvos Respublikos Vyriausybė, Nutarimas
Nr. 390, 2019-04-24, paskelbta TAR 2019-04-26, i. k. 2019-06920
Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo