

Suvestinė redakcija nuo 2024-11-12 iki 2025-06-30

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

Nauja redakcija nuo 2024-11-12:

Nr. [945](#), 2024-11-06, paskelbta TAR 2024-11-11, i. k. 2024-19589

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ
NUTARIMAS
DĖL LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO
ĮGYVENDINIMO

2018 m. rugpjūčio 13 d. Nr. 818
Vilnius

Vadovaudamasi Lietuvos Respublikos kibernetinio saugumo įstatymo 7 straipsnio 2 dalies 3 punktu, 11 straipsnio 6 dalimi, 14 straipsnio 1 dalies 1 punktu ir 2 dalimi, 28 straipsnio 6 dalimi, 30 straipsnio 1 dalimi, 37 straipsnio 1 dalimi, 2 dalies 3 punktu, 4, 6, 8 ir 9 dalimis ir įgyvendindama 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyvą (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148, Lietuvos Respublikos Vyriausybė n u t a r i a:

1. Patvirtinti pridedamus:

- 1.1. Nacionalinį kibernetinių incidentų valdymo planą;
- 1.2. Kibernetinio saugumo subjektų identifikavimo pagal specialiuosius kriterijus metodiką;
- 1.3. Kibernetinio saugumo reikalavimų aprašą;
- 1.4. Vykdomo užtikrinimo priemonių taikymo kibernetinio saugumo subjektams tvarkos aprašą;
- 1.5. Saugiojo valstybinio duomenų perdavimo tinklo naudotojų sąrašą;
- 1.6. Atlyginimo už naudojimąsi Saugiuoju valstybiniu duomenų perdavimo tinklu teikiamomis papildomomis elektroninių ryšių ir kibernetinio saugumo paslaugomis dydžių nustatymo kriterijų ir atlyginimo apskaičiavimo tvarkos aprašą.

2. Įgalioti:

2.1. krašto apsaugos ministrą patvirtinti:

2.1.1. Saugiuoju valstybiniu duomenų perdavimo tinklu teikiamų elektroninių ryšių ir kibernetinio saugumo paslaugų teikimo sąlygas ir taisykles;

2.1.2. Saugiojo valstybinio duomenų perdavimo tinklo naudotojų prisijungimo prie Saugiojo valstybinio duomenų perdavimo tinklo ir atsijungimo nuo jo sąlygas, planą ir terminus, jungimosi prie viešųjų elektroninių ryšių tinklų ne per Saugųjį valstybinį duomenų perdavimo tinklą atvejų sąrašą ir tvarkos aprašą;

2.2. Lietuvos Respublikos krašto apsaugos ministeriją vertinti, ar atlyginimo už naudojimąsi Saugiuoju valstybiniu duomenų perdavimo tinklu teikiamomis papildomomis elektroninių ryšių ir kibernetinio saugumo paslaugomis dydžiai nustatyti atsižvelgiant į atlyginimo už naudojimąsi

Saugiuoju valstybiniu duomenų perdavimo tinklu teikiamomis papildomomis elektroninių ryšių ir kibernetinio saugumo paslaugomis dydžių nustatymo kriterijus, ir teikti išvadą Saugiojo valstybinio duomenų perdavimo tinklo tvarkytojui;

2.3. Nacionalinį kibernetinio saugumo centrą prie Krašto apsaugos ministerijos teikti išvadas krašto apsaugos ministrui dėl valstybės ir savivaldybių institucijų ir įstaigų, valstybės valdomų įmonių ir viešųjų įstaigų (toliau – institucijos) priskyrimo prie būtinų nacionaliniam saugumui, gynybai ar gyvybiškai svarbioms valstybės funkcijoms užtikrinti institucijų.

3. Pavesti kibernetinio saugumo subjektams per 12 mėnesių nuo jų įregistravimo Kibernetinių saugumo subjektų registre pritaikyti kibernetinio saugumo įvykių ir kibernetinių incidentų valdymo tinklą ir informacines sistemas taip, kad kibernetiniai incidentai Kibernetinio saugumo informacinėje sistemoje veikiančioje Nacionalinėje kibernetinių incidentų valdymo platformoje būtų registruojami automatinio būdu. Kibernetinio saugumo subjektui dėl objektyvių priežasčių nespėjus įgyvendinti šiame punkte nustatyto reikalavimo ir pateikus motyvuotą prašymą, Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos turi teisę vieną kartą pratęsti terminą, bet ne ilgiau kaip 12 mėnesių.

Ministras Pirmininkas

Saulius Skvernelis

Krašto apsaugos ministras

Raimundas Karoblis

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2018 m. rugpjūčio 13 d. nutarimu Nr. 818
(Lietuvos Respublikos Vyriausybės
2024 m. lapkričio 6 d. nutarimo Nr. 945
redakcija)

NACIONALINIS KIBERNETINIŲ INCIDENTŲ VALDYMO PLANAS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Nacionalinis kibernetinių incidentų valdymo planas (toliau – Planas) nustato kibernetinių incidentų valdymą, poveikio vertinimą ir informavimą apie juos.

2. Plane vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatyme, Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Europos Parlamento ir Tarybos 2019 m. balandžio 17 d. reglamente (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013.

II SKYRIUS KIBERNETINIŲ INCIDENTŲ VALDYMAS

3. Kibernetinių incidentų valdymo organizavimą kibernetinio saugumo subjekto lygmeniu užtikrina kibernetinio saugumo subjektas. Kibernetinių incidentų valdymo organizavimas užtikrinamas vykdant šiuo Vyriausybės nutarimu tvirtinamo Kibernetinio saugumo reikalavimų aprašo 24 ir 25 punktuose numatytas funkcijas ir kibernetinio saugumo subjekto vadovui ar jo įgaliotam asmeniui paskiriant šias funkcijas vykdančius asmenis (toliau – Saugumo operacijų centras). Kibernetinio saugumo subjektas užtikrina, kad Saugumo operacijų centro funkcijos nebūtų pavedamos kibernetinio saugumo subjekto arba paslaugų teikėjo darbuotojui, atsakingam už tinkamą to kibernetinio saugumo subjekto tinklų ir (ar) informacinių sistemų veiklą.

4. Kibernetinio saugumo subjektas kibernetinių incidentų valdymą organizuoja pagal kibernetinio saugumo subjekto patvirtintą kibernetinių incidentų valdymo planą. Šis planas privalo apimti Tipinio kibernetinių incidentų valdymo proceso schema (Plano 1 priedas) ir Tipiniame kibernetinių incidentų valdymo proceso aprašyme (Plano 2 priedas) numatytus dalyvius, etapus, veiksmus, terminus ir rezultatus.

5. Kibernetinis incidentas laikomas suvaldytu, kai yra atkurtos kibernetinio saugumo subjektų tinklų ir informacinėmis sistemomis teikiamos paslaugos.

6. Nacionaliniu lygmeniu kibernetinių incidentų valdymą pagal Nacionalinio kibernetinių incidentų valdymo proceso schemą (Plano 3 priedas) ir aprašymą (Plano 4 priedas) užtikrina Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC).

7. NKSC, pagal kibernetinio saugumo subjekto prašymą sprendamas dėl resursų skyrimo dideliame kibernetiniame incidentui valdyti, sprendimą priima įvertinęs tikimybę, kad didelis kibernetinis incidentas taps ekstremaliojo įvykiu. Prioritetas skiriamas kibernetiniams incidentams, kurių padariniai labiausiai atitinka arba daugiausiai viršija Vyriausybės nustatytus ekstremaliojo įvykio kriterijus.

8. Įvykus arba kilus grėsmei įvykti dideliame kibernetiniame incidentui, atitinkančiam ekstremaliojo įvykio kriterijus, NKSC apie tai informuoja Vyriausybės kanceliarijos Nacionalinį krizių valdymo centrą (toliau – NKVC).

III SKYRIUS

KIBERNETINIŲ INCIDENTŲ POVEIKIO VERTINIMAS IR INFORMAVIMAS APIE KIBERNETINIUS INCIDENTUS

9. Jei Europos Komisijos įgyvendinamieji teisės aktai neapibrėžia išsamiau, laikoma, kad įvyko didelis kibernetinis incidentas, kaip jis suprantamas pagal Kibernetinio saugumo įstatymo 18 straipsnio 2 dalį, kai:

9.1. kibernetinio saugumo subjektas patiria ar gali patirti didelių paslaugų teikimo sutrikimų ir kibernetinis incidentas atitinka bent vieną iš šių kriterijų:

9.1.1. paslaugos trikdomos visoje Lietuvos teritorijoje ir (ar) bent vienoje Europos Sąjungos arba NATO šalyje;

9.1.2. tinklų ir informacinės sistemos veikla trikdoma 2 ar daugiau valandų;

9.1.3. paveiktų paslaugų gavėjų ar kompiuterizuotų darbo vietų skaičius lygus arba didesnis nei 1 000, arba 25 procentai (atsižvelgiant į tai, kuris dydis yra mažesnis);

9.1.4. paveikti 1 000 arba 25 procentų (atsižvelgiant į tai, kuris dydis yra mažesnis) paslaugų gavėjų asmens duomenys ar kiti kibernetinio saugumo subjekto saugomi paslaugų gavėjų duomenys;

9.1.5. kibernetinio saugumo subjektas nebegali užtikrinti teisės aktuose jo veiklai nustatytų reikalavimų įgyvendinimo;

9.1.6. prarastos arba atskleistos komercinės paslaptys arba įslaptinta informacija;

9.1.7. per 6 mėnesius patiriamas daugiau nei vienas analogiškas kibernetinis incidentas, incidentų pagrindinė priežastis sutampa, o finansinių nuostolių dydis siekia 9.2 papunktyje numatytas vertes;

9.2. kibernetinio saugumo subjektas patiria ar gali patirti didelių finansinių nuostolių, lygių arba didesnių nei 500 000 Eur, arba 5 procentų kibernetinio saugumo subjekto praėjusių finansinių metų apyvartos (atsižvelgiant į tai, kuri suma yra mažesnė);

9.3. kibernetinis incidentas paveikė arba gali paveikti kitus fizinius ar juridinius asmenis, sukeldamas didelę turtinę arba neturtinę žalą, atitinkančią bent vieną iš šių kriterijų:

9.3.1. galimos turtinės žalos dydis yra lygus arba didesnis nei 400 bazinių socialinių išmokų;

9.3.2. galimos neturtinės žalos dydis lygus arba didesnis nei 10 000 Eur;

9.3.3. sutrikdyta bent vieno žmogaus sveikata arba bent vienas žmogus žuvo.

10. Kibernetinio saugumo subjekto Saugumo operacijų centras apie kibernetinius incidentus informuoja NKSC, juos registruodamas Kibernetinio saugumo informacinės sistemos posistemyje – Nacionalinėje kibernetinių incidentų valdymo platformoje (toliau – Platforma).

11. Kibernetinio saugumo subjekto Saugumo operacijų centras, dėl kibernetinio incidento neturintis galimybės apie kibernetinius incidentus informuoti automatizuotu būdu per Platformą, NKSC informuoja užpildydamas formą Platformoje, NKSC interneto svetainėje, NKSC nurodytu elektroninio pašto adresu arba telefonu.

12. Kibernetinio saugumo subjekto Saugumo operacijų centras apie didelį kibernetinį incidentą NKSC informuoja Kibernetinio saugumo įstatymo 18 straipsnio 4 dalyje nustatytais terminais pateikdamas toje pačioje dalyje nurodytą informaciją. Kibernetinio saugumo subjekto Saugumo operacijų centras turi teisę teikti ir kitą, Kibernetinio saugumo įstatymo 18 straipsnio 4 dalyje nenurodytą, tačiau dideliame kibernetiniame incidentui suvaldyti ar tirti reikšmingą informaciją.

13. Kibernetinio saugumo subjekto Saugumo operacijų centras apie kitus kibernetinius incidentus, neatitinkančius Kibernetinio saugumo įstatymo 18 straipsnio 2 dalies ir Plano 9 punkto nuostatų (toliau – nedidelis kibernetinis incidentas), NKSC informuoja pateikdamas:

13.1. nedelsdamas, bet ne vėliau kaip per 72 valandas nuo sužinojimo apie kibernetinį incidentą momento, pranešimą apie nedidelį kibernetinį incidentą, jame pateikdamas Kibernetinio saugumo įstatymo 18 straipsnio 4 dalies 2 punkte nurodytą informaciją;

13.2. per vieną mėnesį nuo pranešimo apie kibernetinį incidentą registravimo dienos galutinę ataskaitą apie nedidelį kibernetinį incidentą, joje pateikdamas Kibernetinio saugumo įstatymo 18 straipsnio 4 dalies 4 punkte nurodytą informaciją. Galutinė ataskaita apie nedidelį kibernetinį incidentą neteikiama, jei pranešime apie kibernetinį incidentą pateikta visa galutinės ataskaitos informacija.

14. Kibernetinio saugumo subjekto Saugumo operacijų centras, teikdamas NKSC Kibernetinio saugumo įstatymo 18 straipsnio 2 dalyje nurodytą informaciją apie kibernetinio incidento pradinį vertinimą, įvardija:

14.1. kokių paslaugų sutrikimų patyrė ar gali patirti kibernetinio saugumo subjektas – nurodomos paslaugos ir sutrikimų apimtys;

14.2. kokių finansinių nuostolių patyrė ar gali patirti kibernetinio saugumo subjektas – nurodomas nuostolių dydis;

14.3. ar kibernetinis incidentas paveikė arba gali paveikti kitus asmenis, sukeldamas turtinę arba neturtinę žalą, – jei taip, nurodomi asmenys ir žalos dydis;

14.4. neteisėtų ar piktavališkų veiksmų įrodymus (jei tokių yra);

14.5. ar incidentas suvaldytas;

14.6. kitą svarbią informaciją (pavyzdžiui, kibernetinio incidento vietą, tikslų nustatymo laiką).

15. Jei kibernetinis incidentas tęsiasi ilgiau nei vieną mėnesį, kibernetinio saugumo subjektai kas mėnesį atnaujina Kibernetinio saugumo įstatymo 18 straipsnio 4 dalies 2 punkte nurodytą informaciją.

16. NKSC prašymu kibernetinio saugumo subjektas NKSC nurodytais terminais privalo teikti tarpines atitinkamų atnaujintų padėties duomenų ataskaitas apie didelius kibernetinius incidentus. NKSC turi teisę paprašyti pateikti ir kitus dideliame kibernetiniame incidentui suvaldyti reikalingus ir reikšmingus duomenis.

17. Asmenys, neturintys pareigos NKSC pranešti apie kibernetinius incidentus, apie kibernetinius incidentus, kibernetines grėsmes, vos neįvykusius kibernetinius incidentus ir (ar) taikytas kibernetinių incidentų valdymo priemonės NKSC savanoriškai praneša:

17.1. kibernetinio saugumo subjekto Saugumo operacijų centras – tokia pat tvarka, kaip ir apie kibernetinius incidentus;

17.2. asmenys, kurie nėra kibernetinio saugumo subjektai – NKSC interneto svetainėje skelbiamais būdais.

18. Teikiant Kibernetinio saugumo įstatymo 18 straipsnio 4 dalies 4 punkto b papunktyje nurodytą informaciją, parenkama viena iš išvardytų kibernetinių grėsmių ir pagrindinių incidentų priežasčių:

18.1. nepageidaujamų laiškų ir (ar) klaidinančios ar žeidžiančios informacijos platinimas (angl. *abusive content, spam*) ir (ar) tinklų informacinės sistemos veiklos trikdymas;

18.2. kenkimo programinė įranga (angl. *malicious software / code*): programinė įranga ar jos dalis, kuri padeda neteisėtai prisijungti prie tinklų ir informacinės sistemos, ją užvaldyti ir kontroliuoti, sutrikdyti ar pakeisti jos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti skaitmeninius duomenis, panaikinti ar apriboti galimybę jais naudotis ir neteisėtai pasisavinti ar kitaip panaudoti neviešus skaitmeninius duomenis tokios teisės neturintiems asmenims ir kuri identifikuota kaip:

18.2.1. pažangi kenkimo programinė įranga (angl. *advanced persistent threat, APT*);

18.2.2. tinklų ir informacinės sistemos duomenis šifruojantis ir naikinantis (angl. *wiper*) ar išpirkos reikalaujantis programinis kodas (angl. *ransomware*);

18.2.3. tinklų ir informacinės sistemos dalys, aktyviai kontroliuojamos įsibrovėlių;

18.2.4. kenkimo programinės įrangos platinimas;

18.3. informacijos rinkimas (angl. *information gathering*): žvalgyba ar kita įtartina veikla, 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. Naudojami socialinės inžinerijos metodai, siekiant išvilioti prisijungimo prie tinklų ir informacinės sistemos ir (ar) kitą svarbią informaciją;

18.4. mėginimas įsilaužti (angl. *intrusion attempts*). Mėginimas įsilaužti arba sutrikdyti tinklų ir informacinės sistemos veikimą išnaudojant žinomas spragas (angl. *exploiting of known vulnerabilities*), bandant parinkti slaptažodžius (angl. *login attempts*), kitą įsilaužimo būdą (angl. *new attack signature*), kurie gali būti skirstomi į:

18.4.1. išnaudojama viena ar kelios nežinomos spragos (angl. *zero day*);

18.4.2. tinklų ir informacinės sistemos žvalgyba ar kita kenkimo veika (prievadų skenavimas, slaptažodžių parinkimas, kenkimo programinės įrangos platinimas ir kita);

18.4.3. išnaudojamos žinomos ir viešai publikuotos spragos;

18.5. įsilaužimas (angl. *intrusions*). Sėkmingas įsilaužimas ir (ar) neteisėtas tinklų ir informacinės sistemos, taikomosios programinės įrangos ar paslaugos naudojimas (angl. *privileged account compromise, unprivileged account compromise, application compromise*), kuris skirstomas taip:

18.5.1. veiksmai prieš tinklų ir informacinę sistemą ar jos saugumo priemones, informacijos pasisavinimas, naikinimas, tinklų ir informacinės sistemos ar jos dalies pažeidimas, sutrikdantis tinklų ir informacinės sistemos teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomos informacijos ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti tinklų ir informacinės sistemos naudotojų pasitikėjimą jais;

18.5.2. gaunama neteisėta prieiga prie tinklų ir informacinės sistemos, taikomosios programinės įrangos ar paslaugos;

18.6. paslaugų trikdymas, prieinamumo pažeidimai (angl. *availability*): veiksmai, kuriais trikdoma tinklų ir informacinės sistemos veikla, teikiamos paslaugos (angl. *DoS, DDoS*), tinklų ir informacinės sistemos ar jos dalies pažeidimas, sutrikdantis tinklų ir informacinės sistemos ir (ar) jos teikiamas paslaugas, kuris skirstomas taip:

18.6.1. teikiamų paslaugų nutraukimas arba maksimalaus leistino paslaugos neveikimo laiko viršijimas;

18.6.2. teikiamų paslaugų nepertraukiamo teikimo trikdymas, galintis turėti įtakos tvarkomos informacijos ir (ar) teikiamų paslaugų prieinamumui;

18.7. tiekimo grandinės atakos (angl. *supply chain attack*): išnaudojama trečiųjų šalių, teikiančių paslaugas tinklų ir informacinės sistemos valdytojui ir (ar) tvarkytojui, infrastruktūra, siekiant įgauti ar turėti įtaką paslaugos gavėjo tinklų ir informacinės sistemos infrastruktūrai;

18.8. informacijos turinio saugumo pažeidimai (angl. *information content security*): neteisėta prieiga prie informacijos, galinčios turėti įtakos tinklų ir informacinės sistemos veiklai ir (ar) teikiamoms paslaugoms, ar jos neteisėtas keitimas;

18.9. neteisėta veikla, sukčiavimas (angl. *fraud*): vagystė, apgavystė, neteisėtas išteklių (angl. *unauthorized use of resources*), nelegalios programinės įrangos ar autorių teisių (angl. *copyright*) naudojimas, tapatybės klaidojimo, apgavystės ir kiti panašaus pobūdžio incidentai;

18.10. kitos grėsmės ar priežastys.

19. Užregistravus incidentą, informacija apie galimą nusikalstamą veiką ar asmens duomenų apsaugos pažeidimą, naudojantis Platforma, pateikiama atitinkamai Lietuvos policijai ir (ar) Valstybinei duomenų apsaugos inspekcijai. Gavę informaciją apie kibernetinį incidentą,

NKSC ir kitos šiame punkte nurodytos institucijos priima sprendimus dėl tyrimų pagal kompetenciją pradėjimo. Duomenys apie kibernetinius incidentus, reikalingi institucijų tyrimams atlikti, išskyrus ikiteisminio tyrimo duomenis, teikiami ir tvarkomi Platformoje.

20. NKSC, Lietuvos policija ir Valstybinė duomenų apsaugos inspekcija, gavę informacijos apie kibernetinius incidentus arba juos nustatę, nedelsdami, bet ne vėliau kaip per 24 valandas nuo informacijos gavimo ar nustatymo momento kibernetinius incidentus registruoja Platformoje teikdami visą turimą informaciją ir apie tai informuoja kibernetinio saugumo subjektų Saugumo operacijų centrą. Apie institucijų užregistruotus kibernetinius incidentus kibernetinio saugumo subjektų Saugumo operacijų centrai informuojami per Platformą. Kibernetinio saugumo subjekto Saugumo operacijų centras Plane nustatytais terminais privalo pateikti Kibernetinio saugumo įstatymo 18 straipsnio 4 dalies 1 arba 2 punkte nurodytą informaciją.

21. NKSC, įvertinęs Platformoje esančią informaciją apie kibernetinius incidentus ir nustatęs, kad nedidelis kibernetinis incidentas turėtų būti priskirtas dideliame kibernetiniame incidentui, kibernetinį incidentą Platformoje priskiria dideliame kibernetiniame incidentui ir apie tai nedelsdamas, bet ne vėliau kaip per 24 valandas nuo šiame punkte nurodyto incidento nustatymo informuoja kibernetinio saugumo subjektą.

22. Kai didelis kibernetinis incidentas yra susijęs su dviem ar daugiau valstybių narių, NKSC apie didelį kibernetinį incidentą ne vėliau kaip per 24 valandas nuo sužinojimo apie jį momento informuoja kitas paveiktas valstybes nares ir Europos Sąjungos tinklą ir informacijos apsaugos agentūrą (toliau – ENISA).

23. NKSC kas 3 mėnesius teikia ENISA suvestinę ataskaitą, į kurią įtraukiami nuasmeninti ir suvestiniai duomenys apie kibernetinius incidentus, kibernetines grėsmes ir vos neįvykusius kibernetinius incidentus.

24. Informaciją apie didelius kibernetinius incidentus, kibernetinius incidentus, kibernetines grėsmes ir vos neįvykusius kibernetinius incidentus, apie kuriuos pranešė kibernetinio saugumo subjektai, kurie Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka buvo pripažinti ypatingos svarbos subjektais, NKSC praneša NKVC ne vėliau kaip per 24 valandas nuo sužinojimo apie juos momento. Apie užregistruotus didelius kibernetinius incidentus kibernetinio saugumo subjektuose, kurie Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka buvo pripažinti ypatingos svarbos subjektais, NKSC praneša NKVC nedelsdamas, bet ne vėliau kaip per 1 valandą nuo kibernetinio incidento užregistravimo. Suvestinę informaciją apie kibernetinius incidentus, kibernetines grėsmes ir vos neįvykusius kibernetinius incidentus šiame punkte nurodytuose kibernetinio saugumo subjektuose NKSC pateikia NKVC kas 3 mėnesius.

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2018 m. rugpjūčio 13 d. nutarimu Nr. 818
(Lietuvos Respublikos Vyriausybės
2024 m. lapkričio 6 d. nutarimo Nr. 945
redakcija)

KIBERNETINIO SAUGUMO SUBJEKTŲ IDENTIFIKAVIMO PAGAL SPECIALIUOSIUS KRITERIJUS METODIKA

I SKYRIUS BENDROSIOS NUOSTATOS

1. Kibernetinio saugumo subjektų identifikavimo pagal specialiuosius kriterijus metodika (toliau – Metodika) nustato kibernetinio saugumo subjektų identifikavimo pagal specialiuosius kibernetinio saugumo subjektų identifikavimo kriterijus (toliau – specialieji kriterijai), nustatytus Lietuvos Respublikos kibernetinio saugumo įstatymo 11 straipsnio 5 dalyje, tvarką.
2. Metodikos priede nustatytos specialiųjų kriterijų vertės, iš kurių atitikus bent vieną, subjektas priskiriamas esminiam kibernetinio saugumo subjektui (toliau – esminis subjektas) arba svarbiam kibernetinio saugumo subjektui (toliau – svarbus subjektas).
3. Kibernetinio saugumo įstatymo 1 ir 2 prieduose nurodytos institucijos, atsakingos už identifikavimą, taip pat ministerijos, formuojančios politiką ministrams pavestose srityse, kurios neapima Kibernetinio saugumo įstatymo 1 ir 2 prieduose nurodytų sektorių, (toliau – Atsakinga institucija), atsižvelgdamos į specialiuosius kriterijus, gali identifikuoti į jų veiklos sritį patenkančius subjektus.
4. Atsakingos institucijos privalo paskirti asmenis, atsakingus už subjektų identifikavimą, ir pateikti paskirtų atsakingų asmenų kontaktinę informaciją Kibernetinio saugumo informacinės sistemos (toliau – KSIS) duomenų tvarkytojui KSIS nuostatuose nustatyta tvarka.
5. Kibernetinio saugumo subjektų identifikavimas pagal šią Metodiką atliekamas KSIS.
6. Metodikoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Kibernetinio saugumo įstatyme, Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatyme, Lietuvos Respublikos viešojo administravimo įstatyme.

II SKYRIUS KIBERNETINIO SAUGUMO SUBJEKTŲ IDENTIFIKAVIMAS

7. KSIS duomenų tvarkytojas sudaro preliminarų pagal specialiuosius kriterijus identifikuojamų kibernetinio saugumo subjektų sąrašą, kuriame nurodomi KSIS duomenų tvarkytojui žinomi Kibernetinio saugumo įstatymo 13 straipsnio 3 dalyje nurodyti duomenys apie kibernetinio saugumo subjektus, ir apie jo sudarymą informuoja Atsakingas institucijas.
8. Atsakinga institucija ne vėliau kaip per dešimt darbo dienų nuo šios Metodikos 7 punkte nurodyto pranešimo gavimo dienos įvertina preliminarų kibernetinio saugumo subjektų sąrašą, jei nustato trūkumų, sąrašą tikslina ar papildo naujais kibernetinio saugumo subjektais, kurie atitinka specialiuosius identifikavimo kriterijus.

9. Atsakinga institucija, įvertinusi preliminarų kibernetinio saugumo subjektų sąrašą, informuoja subjektą apie jo priskyrimą preliminariam kibernetinio saugumo subjektų sąrašui ir prašo subjekto per dešimt darbo dienų nuo pranešimo gavimo dienos patvirtinti pateiktų duomenų teisingumą arba pateiktus duomenis patikslinti vadovaujantis Metodikos priede nustatytomis specialiųjų kriterijų vertėmis. Pasibaigus dešimties darbo dienų terminui ir nesulaukus subjekto atsakymo, laikoma, kad subjektas sutinka, kad pateikti duomenys teisingi. Subjektas turi teisę prašyti pratęsti atsakymo pateikimo terminą, kurį Atsakinga institucija gali pratęsti vieną kartą ne ilgesniam nei dešimties darbo dienų terminui. Atsakinga institucija turi teisę prašyti subjekto papildomos informacijos, kuri reikalinga preliminariam kibernetinio saugumo subjektų sąrašui tikslinti.

10. Atsakinga institucija ne vėliau kaip per dešimt darbo dienų nuo atsakymo, nurodyto Metodikos 9 punkte, gavimo dienos, jei atsakymas buvo pateiktas, įvertina subjekto atsakymą ir prireikus teikia subjektui pastabas ir pasiūlymus ir prašo subjekto per dešimt darbo dienų nuo pranešimo gavimo dienos patvirtinti pateiktų duomenų teisingumą arba pateiktus duomenis patikslinti.

11. Jeigu subjektą vertinti pradėjusi Atsakinga institucija mano, kad šio subjekto identifikavimas priskirtinas kitos Atsakingos institucijos kompetencijai, ji dėl to kreipiasi į KSIS duomenų tvarkytoją, o jis ne vėliau kaip per penkias darbo dienas nuo kreipimosi gavimo dienos priima sprendimą, kuri Atsakinga institucija turi vertinti subjektą.

12. Atsakinga institucija, užbaigusi preliminarų kibernetinio saugumo subjektų sąrašo ar jo dalies vertinimą, kuris negali trukti ilgiau nei tris mėnesius nuo Aprašo 7 punkte nurodytos informacijos gavimo dienos, apie tai praneša KSIS duomenų tvarkytojui.

13. KSIS duomenų tvarkytojas, gavęs Atsakingos institucijos informaciją apie užbaigtą preliminarų kibernetinio saugumo subjektų sąrašo ar jo dalies vertinimą, įtraukia preliminarų kibernetinio saugumo subjektų sąrašo subjektus į kibernetinio saugumo subjektų sąrašą juos įregistrudamas KSIS.

14. KSIS duomenų tvarkytojas ne rečiau kaip kartą per metus atnaujiną preliminarų kibernetinio saugumo subjektų sąrašą, jei yra pasikeitimų, praneša Atsakingai institucijai. KSIS duomenų tvarkytojas ir Atsakinga institucija toliau vykdo veiksmus, nurodytus šios Metodikos 8 – 13 punktuose.

III SKYRIUS BAIGIAMOSIOS NUOSTATOS

15. Subjekto, atitinkančio specialiuosius kriterijus ir savarankiškai pateikusio duomenis KSIS duomenų tvarkytojui KSIS nuostatuose nustatyta tvarka, duomenys vertinami šios Metodikos II skyriuje nustatyta tvarka.

16. Atsakinga institucija, gavusi pranešimą iš kibernetinio saugumo subjekto arba savarankiškai nustatiusi, kad kibernetinio saugumo subjektas neatitinka specialiųjų identifikavimo kriterijų, praneša KSIS duomenų tvarkytojui ir atnaujiną duomenis apie kibernetinio saugumo subjektą KSIS. Gauti duomenys vertinami KSIS nuostatų nustatyta tvarka.

17. KSIS duomenų tvarkytojas ne rečiau kaip kartą per metus atnaujiną duomenis apie subjektus, veikiančius Kibernetinio saugumo įstatymo 1 ir 2 prieduose nurodytuose sektoriuose ir subsektoriuose, ir apie naujus duomenis informuoja Atsakingą instituciją.

18. Atsakinga institucija ministrui pavestose valdymo srityse ne rečiau kaip kartą per metus KSIS atnaujiną duomenis apie subjektus, veikiančius kituose sektoriuose, subsektoriuose,

kurie nėra nurodyti Kibernetinio saugumo įstatymo 1 ir 2 prieduose ir kurie galimai atitinka specialiuosius kibernetinio saugumo subjektų identifikavimo kriterijus.

**KIBERNETINIO SAUGUMO SUBJEKTŲ IDENTIFIKAVIMO PAGAL
SPECIALIUOSIUS KRITERIJUS VERTĖS**

Eil. Nr.	Specialusis identifikavimo kriterijus	Specialiojo identifikavimo kriterijaus vertė identifikuojant esminį subjektą	Specialiojo identifikavimo kriterijaus vertė identifikuojant svarbų subjektą
1.	Subjektas yra vienintelis paslaugos, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ar ekonominės veiklos vykdymą Lietuvos Respublikoje, teikėjas (toliau – vienintelis paslaugos teikėjas)	Subjektas yra vienintelis paslaugos teikėjas, veikiantis bent viename iš Lietuvos Respublikos kibernetinio saugumo įstatymo 1 priede nurodytų sektorių ir subsektorių, ir jo paslaugai teikti yra būtina subjekto valdoma ir (ar) tvarkoma tinklų ir informacinė sistema (toliau – TIS)	1. Subjektas yra vienintelis paslaugos teikėjas, veikiantis bent viename iš Kibernetinio saugumo įstatymo 2 priede nurodytų sektorių ir subsektorių, ir jo paslaugai teikti yra būtina subjekto valdoma ir (ar) tvarkoma TIS. 2. Subjektas yra vienintelis paslaugos teikėjas, veikiantis bent vienoje iš ministrams pavestų valdymo sričių, kurių neapima Kibernetinio saugumo įstatymo 1 ir 2 prieduose nurodyti sektoriai, ir jo paslaugai teikti yra būtina subjekto valdoma ir (ar) tvarkoma TIS
2.	Paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai	Paslaugos, kurią teikia subjektas ir kuriai teikti yra būtina subjekto valdoma ir (ar) tvarkoma TIS, sutrikimas galėtų sukelti ekstremalųjį įvykį, kuris yra apibūdinamas pagal ekstremaliojo įvykio kriterijus	Paslaugos, kurią teikia subjektas ir kuriai teikti yra būtina subjekto valdoma ir (ar) tvarkoma TIS, sutrikimas galėtų sukelti ypatingąjį įvykį
3.	Paslaugos, kurią teikia subjektas, sutrikimas galėtų kelti didelę sisteminę riziką	Paslaugos, kurią teikia subjektas ir kuriai teikti yra būtina subjekto valdoma ir (ar) tvarkoma TIS, sutrikimas	Paslaugos, kurią teikia subjektas ir kuriai teikti yra būtina subjekto valdoma ir (ar) tvarkoma TIS, sutrikimas

Eil. Nr.	Specialusis identifikavimo kriterijus	Specialiojo identifikavimo kriterijaus vertė identifikuojant esminį subjektą	Specialiojo identifikavimo kriterijaus vertė identifikuojant svarbų subjektą
	sektoriuose, kuriuose toks sutrikimas galėtų daryti tarpvalstybinį poveikį	galėtų daryti neigiamą poveikį bent vienai Europos Sąjungos ir (ar) Šiaurės Atlanto sutarties organizacijos (toliau – NATO) valstybei narei ir sukelti paslaugos nepasiekiamumą	galėtų daryti neigiamą poveikį ne Europos Sąjungos ir (ar) NATO valstybei narei ir sukelti paslaugos nepasiekiamumą
4.	Subjektas yra ypatingos svarbos atsižvelgiant į jo konkrečią svarbą konkrečiam sektoriui ar paslaugos rūšiai arba kitiems tarpusavyje priklausomiems sektoriams nacionaliniu ar regioniniu lygmeniu	Subjektas nacionaliniu lygmeniu vykdo ūkinę veiklą bent vienoje srityje, kuri laikoma nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi pagal Lietuvos Respublikos Vyriausybės 2018 m. birželio 6 d. nutarimą Nr. 556 „Dėl ūkinės veiklos sričių, kurios laikomos nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi, sąrašo nustatymo“, ir jo veiklai vykdyti yra būtina subjekto valdoma ir (ar) tvarkoma TIS	Subjektas regioniniu lygmeniu vykdo ūkinę veiklą bent vienoje srityje, kuri laikoma nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi pagal Lietuvos Respublikos Vyriausybės 2018 m. birželio 6 d. nutarimą Nr. 556 „Dėl ūkinės veiklos sričių, kurios laikomos nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi, sąrašo nustatymo“, ir jo veiklai vykdyti yra būtina subjekto valdoma ir (ar) tvarkoma TIS
5.	Subjektas Kibernetinio saugumo įstatymo 1 priede nurodytame viešojo administravimo sektoriuje teikia paslaugas ir (ar) vykdo veiklą, kuriai sutrikus galėtų būti didelis poveikis valstybei, institucijoms ar gyventojams, ir yra laikomas teritoriniu valstybinio	Teritorinis valstybinio administravimo subjektas, kuris valdo ir (ar) tvarko TIS, kurios sutrikimas galėtų sukelti paslaugos nepasiekiamumą ilgiau nei 24 valandas ar daugiau nei 145 tūkst. gyventojų, ar visos savivaldybės gyventojams	–

Eil. Nr.	Specialusis identifikavimo kriterijus	Specialiojo identifikavimo kriterijaus vertė identifikuojant esminį subjektą	Specialiojo identifikavimo kriterijaus vertė identifikuojant svarbų subjektą
	administravimo subjektu ar regioniniu administravimo subjektu, ar savivaldybių administravimo subjektu pagal Lietuvos Respublikos viešojo administravimo įstatymą		
6.	Paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį esminio subjekto teikiamai paslaugai ir (ar) vykdomai veiklai	1. Subjektas teikia TIS (ar jų dalies) nuomos paslaugą esminiam subjektui, numatyta paslaugos teikimo trukmė yra ilgesnė nei 12 mėn., ši TIS (jų dalis) yra būtina esminio subjekto teikiamai paslaugai ir (ar) vykdomai veiklai vykdyti. 2. Subjektas teikia paslaugą, kurios numatyta teikimo trukmė yra ilgesnė nei 12 mėn. ir kuria suteikiama teisė gauti prieigą prie esminio subjekto valdomos ir (ar) tvarkomos TIS (ar jų dalių)	Subjektas teikia paslaugą, kurios numatyta teikimo trukmė yra ilgesnė nei 12 mėn. ir kuria suteikiama teisė aptarnauti esminio subjekto valdomą ir (ar) tvarkomą TIS (ar jų dalis)
7.	Subjektas yra paslaugos, kuri būtina gyvybiškai svarbioms valstybės funkcijoms atlikti ir valstybinėms mobilizacinėms užduotims vykdyti, teikėjas	Subjektas yra paslaugos, kuri būtina gyvybiškai svarbioms valstybės funkcijoms atlikti, teikėjas, jo paslaugai teikti yra būtina subjekto valdoma ir (ar) tvarkoma TIS ir tokiam subjektui Lietuvos Respublikos mobilizacijos ir priimančiosios šalies paramos įstatyme ir jį įgyvendinančiuose teisės aktuose nustatyta tvarka ir sąlygomis pavesta teikti šią	Subjektas yra paslaugos, kuri būtina valstybinėms mobilizacinėms užduotims vykdyti, teikėjas, jo paslaugai teikti yra būtina subjekto valdoma ir (ar) tvarkoma TIS ir tokiam subjektui Lietuvos Respublikos mobilizacijos ir priimančiosios šalies paramos įstatyme ir jį įgyvendinančiuose teisės aktuose nustatyta tvarka ir sąlygomis pavesta teikti

Eil. Nr.	Specialusis identifikavimo kriterijus	Specialiojo identifikavimo kriterijaus vertė identifikuojant esminį subjektą	Specialiojo identifikavimo kriterijaus vertė identifikuojant svarbų subjektą
		paslaugą siekiant užtikrinti atitinkamos gyvybiškai svarbios valstybės funkcijos vykdymą	paslaugą, būtiną valstybinėms mobilizacinėms užduotims vykdyti
8.	Subjektas Kibernetinio saugumo įstatymo 2 priede nurodytame mokslinių tyrimų sektoriuje vykdo ypatingos svarbos mokslinių tyrimų ir eksperimentinės plėtros veiklą		Subjektas Kibernetinio saugumo įstatymo 2 priede nurodytame mokslinių tyrimų sektoriuje vykdo mokslinių tyrimų ir eksperimentinės plėtros veiklą srityse, kurios laikomos nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi, ir jo veiklai vykdyti yra būtina subjekto valdoma ir (ar) tvarkoma TIS

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2018 m. rugpjūčio 13 d. nutarimu Nr. 818
(Lietuvos Respublikos Vyriausybės
2024 m. lapkričio 6 d. nutarimo Nr. 945
redakcija)

KIBERNETINIO SAUGUMO REIKALAVIMŲ APRAŠAS

I SKYRIUS

BENDROSIOS NUOSTATOS

1. Kibernetinio saugumo reikalavimų apraše (toliau – Aprašas) nustatomi kibernetinio saugumo subjektams taikomi kibernetinio saugumo reikalavimai.

2. Apraše vartojamos sąvokos apibrėžtos Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos viešųjų pirkimų įstatyme ir Lietuvos standarte LST EN ISO/IEC 27002.

3. Kibernetinio saugumo subjektas, įgyvendindamas Aprašo reikalavimus, susijusius su dokumentų tvirtinimu, turi teisę pasirinkti nurodytus reikalavimus įgyvendinančias nuostatas dėstyti viename dokumente arba išdėstyti jas atskiruose dokumentuose.

II SKYRIUS

KIBERNETINIO SAUGUMO REIKALAVIMAI

PIRMASIS SKIRSNIS

TINKLŲ IR INFORMACINIŲ SISTEMŲ SAUGUMO POLITIKA

4. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi patvirtinti tinklų ir informacinių sistemų kibernetinio saugumo politikos dokumentą, kuriame turi būti nustatyta:

4.1. veiklos užtikrinant kibernetinį saugumą tikslai, suformuluoti pagal Kibernetinio saugumo įstatyme nustatytus kibernetinio saugumo principus;

4.2. kibernetinį saugumą reglamentuojančių teisės aktų, kuriais vadovaujamasi, sąrašas;

4.3. kiti kibernetinio saugumo politikos dokumentai, kuriais vadovaujamasi įgyvendinant tinklų ir informacinių sistemų saugumo politiką;

4.4. kibernetinio saugumo politikos įpareigojimai, kurių turi laikytis darbuotojai ir trečiosios šalys;

4.5. įsipareigojimai reguliariai, ne rečiau kaip kartą per metus arba pasikeitus aplinkybėms, peržiūrėti ir atnaujinti kibernetinio saugumo politikos dokumentus.

5. Kibernetinio saugumo subjektai turi pateikti ir (ar) atnaujinti kibernetinio saugumo politikos dokumento (-ų) patvirtinimo duomenis, nurodymai dokumento pavadinimą, patvirtinimo datą ir registracijos numerį, Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – NKSC) į Kibernetinio saugumo informacinę sistemą (toliau – KSIS) ne vėliau kaip per 5 darbo dienas nuo šio dokumento (-ų) patvirtinimo ir (ar) pakeitimo dienos.

6. NKSC, atlikdamas kibernetinio saugumo subjekto patikrinimą, turi teisę pareikalauti pateikti Aprašo 3 punkte nurodytų dokumentų kopijas į KSIS ne vėliau kaip per 5 darbo dienas nuo NKSC prašymo gavimo dienos.

ANTRASIS SKIRSNIS

KIBERNETINIO SAUGUMO RIZIKOS ANALIZĖ

7. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi nustatyti kibernetinio saugumo subjekto tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarką, apimančią:

7.1. už rizikos vertinimą, rizikos vertinimo proceso priežiūrą bei nuolatinį tobulinimą atsakingo asmens arba asmenų paskyrimą;

7.2. vertinimo ir valdymo procesą;

7.3. priimtina kibernetinio saugumo subjektui rizikos lygį;

7.4. rizikos vertinimo periodiškumo reikalavimus.

8. Rizikos vertinimo ir valdymo procesas turi apimti bent šiuos elementus:

8.1. tinklų ir informacinių sistemų identifikavimą ir klasifikavimą;

8.2. rizikos analizę, apimančią grėsmių ir spragų analizę ir vertinimą, galimą poveikį, rizikos apskaičiavimą;

8.3. rizikos valdymo priemonių pasirinkimą.

9. Rizikos vertinimas turi būti atliekamas ne rečiau kaip kartą per metus, įvykus esminiams kibernetinio saugumo subjekto organizaciniais ar kitiems reikšmingiems pokyčiams, taip pat įvykus dideliu kibernetiniam incidentui.

10. Atlikus rizikos vertinimą, kibernetinio saugumo subjektai turi parengti rizikos vertinimo ataskaitą ir, jei rizikos vertinimo metu yra nustatoma šalinamų trūkumų, rizikos valdymo planą, kuriuos patvirtina kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo.

11. Rizikos vertinimo ataskaita turi apimti bent tinklų ir informacinių sistemų turto identifikavimą, poveikio vertinimą, grėsmių ir spragų vertinimo informaciją bei rizikos apskaičiavimo rezultatus pagal kibernetinio saugumo subjekto nustatytus kriterijus, taip pat rizikos valdymą.

12. Rizikos valdymo planas turi apimti bent priemonių nepriimtinioms rizikoms valdyti nustatymą ir reikalingus išteklius, už priemonių įgyvendinimą atsakingus asmenis bei priemonių įgyvendinimo terminus.

13. Kibernetinio saugumo subjektas teikia rizikos vertinimo ataskaitos ir rizikos valdymo plano patvirtinimo duomenis, nurodydamas patvirtinimo datą ir registracijos numerį bei rizikos vertinimo metu nustatytus apibendrintus rezultatus: identifikuotas grėsmės, jų tikimybę ir poveikį veiklai, rizikos lygius ir valdymo priemonės, į KSIS ne vėliau kaip per 5 darbo dienas nuo šių dokumentų patvirtinimo.

14. Kibernetinio saugumo subjekto vadovo arba jo įgalioto asmens patvirtintos rizikos vertinimo ataskaitos ir rizikos valdymo planai turi būti saugomi ne mažiau kaip 3 metus.

15. NKSC, atlikdamas kibernetinio saugumo subjekto patikrinimą, turi teisę pareikalauti kibernetinio saugumo subjekto pateikti rizikos vertinimo ataskaitos kopiją ir rizikos valdymo priemonių plano kopiją. Kibernetinio saugumo subjektas šiuos dokumentus turi pateikti į KSIS ne vėliau kaip per 5 darbo dienas nuo NKSC prašymo gavimo dienos.

TREČIASIS SKIRSNIS

UŽ KIBERNETINĮ SAUGUMĄ ATSAKINGŲ ASMENŲ IR KIBERNETINIO SAUGUMO SUBJEKTO VADOVO AR JO ĮGALIOTO ASMENS PAREIGOS

16. Kibernetinio saugumo subjekto vadovas ar jo įgaliotas asmuo turi paskirti už kibernetinį saugumą atsakingus asmenis, nurodytus Kibernetinio saugumo įstatymo 15 straipsnyje, ir kitus už Aprašo reikalavimų įgyvendinimą atsakingus asmenis.

17. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi užtikrinti, kad NKSC būtų informuotas apie paskirtus už kibernetinį saugumą atsakingus asmenis per KSIS ir būtų pateikta KSIS nuostatuose nurodyto turinio kontaktinė informacija.

18. Kibernetinio saugumo subjekto darbuotojai turi būti informuoti apie paskirtus už kibernetinį saugumą atsakingus asmenis.

19. Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis negali vykdyti funkcijų, susijusių su tinklų ar informacinių sistemų administravimu ar kitomis pareigybėmis, susijusiomis su techninės kompiuterinės įrangos ar programinės įrangos priežiūra ir valdymu.

20. Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis, koordinuodami ir prižiūrėdami kibernetinio saugumo politikos dokumentuose nustatytų reikalavimų įgyvendinimą, turi atlikti šias funkcijas:

20.1. organizuoti kibernetinio saugumo subjekto atitikties šio Aprašo reikalavimams vertinimą NKSC patvirtintos Kibernetinio saugumo auditų atlikimo metodikos nustatyta tvarka;

20.2. užtikrinti, kad kibernetinio saugumo politikos dokumentai būtų parengti ir periodiškai atnaujinami remiantis Kibernetinio saugumo įstatymo ir jį įgyvendinančių teisės aktų reikalavimais;

20.3. koordinuoti tinklų ir informacinių sistemų kibernetinių incidentų tyrimus ir bendradarbiauti su kompetentingomis institucijoms, tiriančiomis kibernetinius incidentus bei neteisėtas veikas, susijusias su kibernetiniais incidentais;

20.4. teikti tinklų ir informacinių sistemų administratoriui (-iams) ir (ar) naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su kibernetinio saugumo politikos dokumentuose nustatytų reikalavimų įgyvendinimu;

20.5. organizuoti rizikos vertinimą ir dalyvauti rizikos vertinimo procese, rengti ir teikti tvirtinti kibernetinio saugumo subjekto vadovui ar jo įgaliotam asmeniui rizikos vertinimo ataskaitas ir rizikos valdymo planus;

20.6. organizuoti darbuotojų mokymus kibernetinio saugumo klausimais;

20.7. atlikti kitas kibernetinio saugumo politikos dokumentuose ir kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir jam priskirtas funkcijas.

21. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi paskirti atsakingą asmenį (administratorių) tinklams ir (ar) informacinėms sistemoms prižiūrėti, jų veikimui užtikrinti. Šio asmens funkcijos turi apimti tinklų ir informacinių sistemų naudotojų prieigos teisių valdymą, tinklų ir informacinių sistemų komponentų (kompiuterių, operacinių sistemų, duomenų bazių, taikomųjų programų, saugasienių, įsibrovimo aptikimo sistemų) priežiūrą, šių informacinės sistemos komponentų sąranką, informacinių sistemų pažeidžiamų vietų nustatymą, saugumo reikalavimų atitikties nustatymą ir stebėseną, reagavimą į kibernetinius incidentus.

KETVIRTASIS SKIRSNIS

KIBERNETINIŲ INCIDENTŲ VALDYMAS

22. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi patvirtinti kibernetinių incidentų valdymo planą, kuris turi atitikti Lietuvos Respublikos Vyriausybės patvirtinto Nacionalinio kibernetinių incidentų valdymo plano nuostatas.

23. Tais atvejais, kai kibernetinio saugumo subjektui tinklų ir informacinių sistemų paslaugas, susijusias su kibernetinių incidentų valdymu, teikia paslaugų teikėjai, kibernetinio saugumo subjekto kibernetinių incidentų valdymo planas turi būti suderintas su paslaugų teikėju.

24. Kibernetinių incidentų valdymo plane turi būti nurodyta:

- 24.1. kibernetinių incidentų nustatymo būdai;
- 24.2. kibernetinių incidentų vertinimas;
- 24.3. kibernetinių incidentų valdymo organizavimas;
- 24.4. kibernetinių incidentų komunikavimo su suinteresuotomis šalimis nuostatos;
- 24.5. darbuotojų, kurie yra atsakingi už kibernetinių incidentų valdymą, atsakomybė;
- 24.6. kibernetinių incidentų įrodymų nustatymo, rinkimo, gavimo, pranešimo ir išsaugojimo nuostatos;
- 24.7. įgytos kibernetinių incidentų valdymo patirties vertinimas;
- 24.8. kibernetinių incidentų valdymo plano veiksmingumo išbandymo ir išbandymo rezultatų ataskaitų rengimo nuostatos.

25. Kibernetinio saugumo subjektas turi nustatyti žurnalinių įrašų (angl. *log*) administravimo ir saugojimo, įsibrovimų aptikimo ir prevencijos reikalavimus, kuriuose turi būti nustatyta:

25.1. operacinių sistemų, tinklų ir informacinių sistemų, techninės įrangos žurnalinių įrašų saugojimo, fiksavimo ir analizės periodiškumo reikalavimai;

25.2. įeinančio ir išeinančio tinklo duomenų srauto, antivirusinės programinės įrangos, įsibrovimų aptikimo ir prevencijos sistemos ar saugasienės žurnalinių įrašų saugojimo fiksavimo ir analizės periodiškumo reikalavimai;

25.3. tinklų ir informacinių sistemų konfigūracinių ir atsarginių kopijų failų prieigos ar pakeitimo veiksmų rinkimo reikalavimai.

26. Kibernetinio saugumo subjektams taikomi techniniai reikalavimai nurodyti 1 lentelėje.

1 lentelė

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
1.	Turi būti fiksuojami bent jau šie žurnaliniai įrašai (jei tinklų ir informacinės sistemos dalys palaiko tokį funkcionalumą):		
1.1.	tinklų ir informacinės sistemos komponentų (serverių, virtualių serverių, saugasienių, maršrutizatorių, komutatorių ir kitų subjekto identifikuotų svarbių komponentų) įjungimas, išjungimas ar perkrovimas;	x	x
1.2.	naudotojų ir administratorių autentifikavimo įvykiai;	x	x
1.3.	naudotojų, administratorių paskyrų sukūrimas, prieigų prie tinklų ir informacinių sistemų pakeitimai;	x	x
1.4.	administratorių atliekami veiksmai;	x	x
1.5.	operacinėse sistemose sukurti ir atlikti sisteminiai uždavinių įvykiai (angl. <i>Scheduled task</i>);	x	x
1.6.	grupinių politikų pakeitimai;	x	x
1.7.	saugasienių taisyklių pakeitimai;	x	x
1.8.	žurnalinių įrašų rinkimo funkcijos įjungimas, išjungimas;	x	x
1.9.	operacinių sistemų laiko ir datos pakeitimai;	x	
1.10.	saugumo sistemų (antivirusinių, įsibrovimo aptikimo sistemų) įjungimas ir išjungimas;	x	x
1.11.	operacinėse sistemose vykstančių procesų ar servisų įvykiai;	x	x
1.12.	tinklų ir informacinių sistemų galinių įrenginių autentifikavimo įvykiai;	x	x

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
1.13 .	žurnalinių įrašų peržiūrėjimas, trynimas, kūrimas ar keitimas.	x	x
2.	Tinklai ir informacinės sistemos turi turėti ne mažiau kaip 2 laiko šaltinius.	x	x
3.	Žurnaliniuose įrašuose turi būti fiksuojami bent jau šie duomenys (jei tinklų ir informacinės sistemos dalys palaiko tokį funkcionalumą):		
3.1.	įvykio data ir tikslus laikas;	x	x
3.2.	įvykio rūšis (informacija, klaida, saugumo pranešimas, sisteminis pranešimas, perspėjimas (angl. <i>warning</i>));	x	
3.3.	naudotojo / administratoriaus ir (arba) tinklų ir informacinės sistemos įrenginio, susijusio su įvykiu, identifikavimo duomenys;	x	x
3.4.	įvykio aprašymas.	x	x
4.	Priemonės, naudojamos vidinės tinklų ir informacinės sistemos sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad žurnaliniuose įrašuose fiksuotų visus įvykius, susijusius su įeinančiais ir išėinančiais duomenų srautais.	x	x
5.	Tinklų ir informacinės sistemos fiksuojami žurnaliniai įrašai turi būti saugomi specializuotoje tam pritaikytoje techninėje ar programinėje įrangoje.	x	
6.	Dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant (automatiniu pranešimu angl. <i>alert</i>), bet ne vėliau kaip per vieną darbo dieną turi būti informuojamas kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.	x	
7.	Žurnaliniai įrašai turi būti saugomi ne trumpiau kaip 90 kalendorinių dienų.	x	x
8.	Draudžiama žurnalinius įrašus trinti, keisti, kol nesibaigęs žurnalinių įrašų saugojimo terminas.	x	x
9.	Žurnalinių įrašų kopijos turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo.	x	x

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
10.	Naudojimasis žurnaliniais įrašais turi būti kontroliuojamas ir fiksuojamas, žurnaliniai įrašai turi būti pasiekiami tik kibernetinio saugumo subjekto įgaliotiems asmenims ir kibernetinio saugumo vadovui (peržiūros teisėmis).	x	x
11.	Žurnalinių įrašų duomenys turi būti analizuojami įgalioto asmens ne rečiau kaip kartą per mėnesį ir apie analizės rezultatų nuokrypius informuojamas kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.	x	x
12.	Turi būti įdiegtos ir veikti įsibrovimo aptikimo sistemos, kurios stebėtų į tinklą ir informacinę sistemą įeinantį ir iš jos išeinantį duomenų srautą.	x	x
13.	Neįprasta veikla turi būti užfiksuojama žurnaliniuose įrašuose ir, jei įmanoma, automatizuotomis priemonėmis sukuriamas automatinis pranešimas, kurį matytų kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.	x	x
14.	Kibernetinio saugumo subjekto vidinės tinklų ir informacinės sistemos turi būti atskirtos nuo viešųjų ryšių tinklų naudojant saugasienę.	x	x
15.	Saugasienės saugumo taisyklės turi būti nuolat peržiūrimos ir prireikus atnaujinamos. Būtina atlikti detalią taisyklių analizę ne rečiau kaip kartą per 6 mėn.	x	x

PENKTASIS SKIRSNIS VEIKLOS TĘSTINUMAS

27. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi patvirtinti tinklų ir informacinių sistemų veiklos tęstinumo valdymo planą, kuriame turi būti nurodyta:

27.1. sąlygos, kada pradedamas taikyti tinklų ir informacinių sistemų veiklos tęstinumo planas;

27.2. tinklų ir informacinių sistemų veiklos kriterijai, pagal kuriuos galima nustatyti, ar tinklų ir informacinės sistemos veikla atkurta;

27.3. asmenys, atsakingi už tinklų ir informacinių sistemų veiklos tęstinumo plano vykdymą, jų pareigos ir funkcijos;

27.4. nuostatos, kuriose turi būti nurodyti tinklų ir informacinių sistemų veiklos testinumo valdymo grupės sudėties ir jos funkcijų reikalavimai, įtraukiant reikalavimą, kad veiklos testinumo valdymo grupės sudėtyje būtų kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis;

27.5. nuostatos, kuriose turi būti nurodyti tinklų ir informacinių sistemų veiklos atkūrimo grupės sudėties ir jos funkcijų reikalavimai;

27.6. detalus tinklų ir informacinių sistemų veiklos atkūrimo planas;

27.7. tinklų ir informacinių sistemų veiklos testinumo valdymo plano veiksmingumo išbandymo reikalavimai;

27.8. tinklų ir informacinių sistemų veiklos testinumo valdymo plano veiksmingumo išbandymo rezultatų ataskaitų rengimo reikalavimai;

27.9. atsarginių duomenų kopijų atkūrimo parametrai pagal kibernetinio saugumo subjekto nustatytą tinklų ir informacinių sistemų ar jų dalies atkūrimo laikotarpį (angl. *Recovery time objective*, RTO) ir šių parametrų išbandymo reikalavimai;

27.10. tinklų ir informacinių sistemų ar jų dalies duomenų praradimo laikas (angl. *Recovery point objective*, RPO) ir jo išbandymo reikalavimai.

28. Kibernetinio saugumo subjektas turi nustatyti atsarginių duomenų kopijų kūrimo, saugojimo ir duomenų atkūrimo iš jų reikalavimus, apibrėžti atsarginio kopijavimo mastą ir dažnį, atsižvelgdamas į veiklos testinumo valdymo plane nustatytus tinklų ir informacinių sistemų nustatytus atkūrimo reikalavimus (RTO, RPO).

29. Kibernetinio saugumo subjektas teikia tinklų ir informacinių sistemų veiklos testinumo valdymo plano išbandymo ataskaitos patvirtinimo duomenis, nurodydamas patvirtinimo datą ir registracijos numerį, į KSIS ne vėliau kaip per 5 darbo dienas nuo šių dokumentų patvirtinimo.

30. NKSC, atlikdamas kibernetinio saugumo subjekto patikrinimą, turi teisę pareikalausti kibernetinio saugumo subjekto pateikti veiklos testinumo valdymo plano išbandymo ataskaitos kopiją. Kibernetinio saugumo subjektas šiuos dokumentus turi pateikti į KSIS ne vėliau kaip per 5 darbo dienas nuo NKSC prašymo gavimo dienos.

31. Kibernetinio saugumo subjektams taikomi techniniai reikalavimai nurodyti 2 lentelėje.

2 lentelė

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
16.	Turi būti užtikrintas kibernetinio saugumo subjekto įvertintų kaip kritinių veiklos testinumo būtinų tinklų ir informacinių sistemų prieinamumas:		
16.1	ne mažiau kaip 96 proc. laiko;		x

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
16.2	ne mažiau kaip 99 proc. laiko.	x	
17.	Kibernetinio saugumo subjekto nustatyta tvarka ir nustatytu reguliarumu turi būti daromos atsarginės duomenų kopijos (toliau – kopijos) ir turi būti laikomos geografiškai nutolusioje vietoje.	x	x
18.	Kopijos turi būti reguliariai testuojamos įgalioto asmens arba turi būti naudojama speciali programinė įranga, kuri automatiškai patikrina, ar iš duomenų kopijos galima atkurti duomenis, kurie būtų visiškai funkcionalūs.	x	x
19.	Turi būti numatytos atsarginės patalpos, į kurias galima būtų laikinai perkelti tinklų ir informacinių sistemų įrangą, nesant galimybių tęsti veiklos pagrindinėse patalpose, ir jos turi atitikti pagrindinėms patalpoms keliamus reikalavimus.	x	x
20.	Svarbiausia tinklų ir informacinių sistemų įrangą, duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima.	x	x

ŠEŠTASIS SKIRSNIS

TIEKIMO GRANDINĖS SAUGUMAS

32. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi nustatyti tiekimo grandinės saugumo valdymo tvarką, taikomą paslaugų, darbų ar įrangos pirkimams, susijusiems su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu ir (ar) kibernetinio saugumo užtikrinimu, siekiant mažinti galimas kilti rizikas tinklų ir informacinėms sistemoms.

33. Kibernetinio saugumo subjektas, nustatydamas tiekimo grandinės saugumo valdymo tvarką, turi numatyti tinklų ir informacinių sistemų tiekėjų atrankos kriterijus, apimančius:

33.1. tiekėjo atitiktį Apraše nustatytiems kibernetinio saugumo reikalavimams;

33.2. kokybės reikalavimus tinklų ir informacinių sistemų produktams, paslaugoms;

33.3. prieigų valdymą, įskaitant prieigų laikotarpio ribojimą.

34. Kibernetinio saugumo subjektas sutartyse su tiekėjais (įskaitant subtiekejus), kiek tai susiję su teikiamomis paslaugomis, turi numatyti:

34.1. tiekėjo atitikties šiam Aprašui reikalavimus;

34.2. tiekėjo personalui reikalingus įgūdžius ir (ar) mokymus, ir (ar) sertifikatus, ir (ar) kvalifikaciją;

34.3. tiekėjo pareigą pranešti kibernetinio saugumo subjektui apie visus didelius ir (ar) kitus incidentus, susijusius su kibernetinio saugumo subjekto tinklų ir informacinėmis sistemomis, kai tik tiekėjas sužino apie incidentą, ir pateikti kibernetinio saugumo subjektui kibernetinio incidento tyrimo ataskaitą;

34.4. teisę kibernetinio saugumo subjektui arba jo įgaliotiems paslaugų teikėjams atlikti tiekėjo atitikties Aprašui auditą (įskaitant neplaninį) ir tiekėjo pareigą sudaryti sąlygas tokiam auditui atlikti sutarties vykdymo laikotarpiu ar įvykus dideliame incidentui;

34.5. pareigą užtikrinti spragų, keliančių riziką kibernetinio saugumo subjekto tinklams ir informacinėms sistemoms, valdymą;

34.6. konfidencialumo ir duomenų neatskleidimo įsipareigojimus;

34.7. paslaugų teikimo lygmenis (angl. *Service Level Agreement*, SLA);

34.8. apibrėžti tiekėjų prieigos (loginės ir fizinės) prie tinklų ir informacinės sistemos lygius ir sąlygas;

34.9. numatyti reikalavimus, keliamus tiekėjo patalpoms, įrangai, tinklų ir informacinių sistemų priežiūrai, informacijos perdavimui tinklais;

34.10. numatyti tiekėjo ir kibernetinio saugumo subjekto teises ir pareigas.

35. Kibernetinio saugumo subjektas, tvirtindamas tiekimo grandinės saugumo valdymo tvarką, turi numatyti tinklų ir informacinių sistemų paslaugų teikėjų rizikos vertinimo reikalavimus.

36. Esminis kibernetinio saugumo subjektas su interneto paslaugos, jei duomenų perdavimo paslauga yra esminė paslaugai teikti, teikėju turi būti sudaręs sutartį (-is), kurioje (-iose) būtų numatyta:

36.1. reagavimas į kibernetinius incidentus įprastomis darbo valandomis;

36.2. reagavimas į kibernetinius incidentus po darbo valandų;

36.3. nepertraukiamas interneto paslaugos teikimas: 24 valandas per parą, 7 dienas per savaitę;

36.4. paslaugos sutrikimų registravimas: 24 valandas per parą, 7 dienas per savaitę;

36.5. apsaugos nuo tinklų ir informacinės sistemos trikdymo taikymas (angl. *Denial of Service*, DoS).

37. Svarbus kibernetinio saugumo subjektas su interneto paslaugos, jei duomenų perdavimo paslauga yra esminė paslaugai teikti, teikėju turi būti sudaręs sutartį (-is), kurioje (-iose) turi būti numatyta:

37.1. reagavimas į kibernetinius incidentus įprastomis darbo valandomis;

37.2. nepertraukiamas paslaugos teikimas įprastomis darbo valandomis;

37.3. paslaugos sutrikimų registravimas įprastomis darbo valandomis;

37.4. apsaugos nuo tinklų ir informacinės sistemos trikdymo taikymas (DoS).

38. Kibernetinio saugumo subjektas turi vykdyti sutartyje su tiekėju nurodytą kibernetinio saugumo reikalavimų įgyvendinimo kontrolę.

39. Kibernetinio saugumo subjektas turi būti sudaręs tiekėjų sąrašą, jį tvarkyti ir pasikeitus sutartims peržiūrėti ir atnaujinti numatytu periodiškumu ir kai įvyksta reikšmingi pokyčiai arba reikšmingi incidentai, susiję su tiekėjais.

SEPTINTASIS SKIRSNIS

TINKLŲ IR INFORMACINIŲ SISTEMŲ ĮSIGIJIMAS, PLĖTOJIMAS IR PRIEŽIŪROS SAUGUMAS, ĮSKAITANT SPRAGŲ VALDYMĄ IR ATSKLEIDIMĄ

40. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi nustatyti tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo užtikrinimo tvarką, kuri apimtų:

- 40.1. tinklų ir informacinių sistemų įsigijimo ir diegimo reikalavimus;
- 40.2. saugumo sistemų, skirtų tinklams ir informacinėms sistemoms nuo kenkimo programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.) apsaugoti, naudojimo nuostatas ir atnaujinimo reikalavimus;
- 40.3. kompiuterių tinklo filtravimo įrangos (saugasienių, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kita) pagrindines naudojimo nuostatas;
- 40.4. duomenų perdavimo tinklo saugumo užtikrinimo priemonės;
- 40.5. elektroninio pašto saugaus naudojimo nuostatas;
- 40.6. leistinos programinės įrangos sąrašo tvirtinimo, peržiūrėjimo reguliarumo ne rečiau kaip kartą per metus ir atnaujinimo nuostatas;
- 40.7. kitas priemones, naudojamas kibernetiniam saugumui užtikrinti.

41. Programinę įrangą diegia tik kibernetinio saugumo subjekto įgalioti asmenys. Sistemų naudotojai negali būti įgaliojami diegti programinę įrangą savarankiškai.

42. Kibernetinio saugumo subjektas turi nustatyti tinklų ir informacinių sistemų pokyčių (toliau – pokyčiai) valdymo tvarką, apimančią planavimą, pokyčių identifikavimą, skirstymą į kategorijas pagal pokyčio tipą, įtakos vertinimą ir pokyčių prioritetų nustatymą.

43. Visi pokyčiai, galintys sutrikdyti ar sustabdyti kibernetinio saugumo subjekto veiklą, turi būti suderinti su kibernetinio saugumo subjekto vadovu ar jo įgaliotu asmeniu ir turi būti patikrinti bandomojoje aplinkoje.

44. Kibernetinio saugumo subjektas turi nustatyti pataisų valdymo tvarką. Saugos pataisos turi būti testuojamos prieš jas diegiant produkcinėje aplinkoje. Turi būti diegiamos oficialių gamintojų saugos pataisos, prieš pataisų diegimą turi būti atliekamas jų vientisumo tikrinimas. Saugos pataisos nediegiamos, jei jose aptinkama spragų, kurios gali daryti didesnę žalą, nei jų diegimo nauda.

45. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi patvirtinti spragų valdymo ir atskleidimo nuostatas, kuriose turi būti nustatyta:

- 45.1. spragų, galinčių turėti įtakos kibernetiniam saugumui, nustatymas ir vertinimas;
- 45.2. už spragų nustatymą atsakingų asmenų teisės ir pareigos;
- 45.3. spragų nustatymo plano rengimas;
- 45.4. spragų nustatymo programinės įrangos naudojimas;

- 45.5. spragų nustatymo rezultatų klasifikavimas;
- 45.6. spragų nustatymo ataskaitų rengimas ir nustatytų trūkumų šalinimas;
- 45.7. reikalavimas nedelsiant pašalinti spragą, įvertintą kaip itin reikšmingą tinklų ir informacinių sistemų veiklai;
- 45.8. reikalavimas reguliariai vertinti spragas, o visą tinklų informacinės sistemos spragų skenavimą atlikti ne rečiau kaip kas 6 mėnesius;
- 45.9. spragų, apie kurias informacija gauta pagal Kibernetinio saugumo įstatymo 25 straipsnį, tyrimas ir informacijos teikimas.
46. Spragų tvarkymas turi būti suderintas su kibernetinio saugumo subjekto pokyčių ir incidentų valdymo nuostatomis.
47. Kibernetinio saugumo subjektams taikomi techniniai reikalavimai nurodyti 3 lentelėje.

3 lentelė

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
21.	Kibernetinio saugumo subjektas turi turėti aktualią tinklų ir informacinių sistemų infrastruktūros loginę schemą ir visų tinklų ir informacinių sistemų schemas (atnaujinti joms pasikeitus).	x	x
22.	Įsilaužimo atakų pėdsakai (angl. <i>attack signature</i>) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu kibernetinio saugumo subjekto sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio kibernetinio saugumo subjekto veiklai vertinimas (testavimas).	x	
23.	Serveriuose (įskaitant ir virtualias mašinas) ir darbo stotyse turi būti įjungtos ir sukonfigūruotos saugasienės, kurios kontroliuoja visą įeinantį ir išeinantį srautą.	x	x
24.	Iš išorės gaunami elektroniniai laiškai turi būti filtruojami, siekiant aptikti ir blokuoti kenksmingą turinį.	x	x
25.	Techninės ir programinės įrangos, kuri skirta kibernetiniams incidentams aptikti, konfigūracijos taisyklės turi būti saugomos elektronine forma atskirai nuo tinklų ir	x	x

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
	informacinių sistemų techninės įrangos (kartu nurodant atitinkamas datas (įgyvendinimo, atnaujinimo), atsakingus asmenis, taikymo periodus).		
26.	Prisijungiant prie belaidžio tinklo (jeigu jungiamasi prie tinklų ir informacinės sistemos vidinio tinklo), turi būti taikomas tinklų ir informacinių sistemų naudotojų tapatumo patvirtinimo EAP (angl. <i>Extensible Authentication Protocol</i>) / TLS (angl. <i>Transport Layer Security</i>) protokolas arba naujesnis protokolas, visuotinai pripažįstamas saugiu.	x	x
27.	Tinklui valdyti turi būti naudojami saugūs tinklo protokolai.	x	x
28.	Turi būti uždrausti / išjungti visi nebūtini protokolai ir atviri prievadai (angl. <i>port</i>).	x	x
29.	Kompiuteriuose, mobiliuosiuose įrenginiuose turi būti išjungtas lygiarangis (angl. <i>peer to peer</i>) funkcionalumas, jei tai nėra reikalinga darbo funkcijoms atlikti.	x	
30.	Turi būti diegiami naudojamos programinės įrangos gamintojų ir operacinių sistemų rekomenduojami atnaujinimai.	x	x
31.	Tinklų ir informacinės sistemos, dėl objektyvių priežasčių naudojančios nepalaikomas operacinių sistemų ir kitos programinės įrangos versijas, turi veikti atskirame tinklo segmente, atskirtame nuo pagrindinių kibernetinio saugumo subjekto veiklos funkcijų.	x	x
32.	Vidinis kibernetinio saugumo subjekto kompiuterių tinklas turėtų būti segmentuotas, jame atskiriant bent:		
32.1.	tinklų ir informacinių sistemų valdymo ir administravimo potinklį;	x	x
32.2.	atskirą potinklį kiekvienai trečiajai šaliai arba kitais būdais užtikrinant trečiųjų šalių prieigą tik prie tai šaliai reikalingų resursų, kur įmanoma taikant kelių veiksmų prisijungimo autentifikaciją. Prisijungimas turi būti atliekamas naudojant saugų virtualųjį privatų tinklą (angl. <i>Virtual private network</i> , VPN). Prisijungimas registruojamas įvykių registravimo žurnaluose;	x	x

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
32.3.	tinklinių daugiafunkcių įrenginių bei spausdintuvų ir skenerių potinklį;	x	x
32.4.	IP telefonijos potinklį;	x	x
32.5.	darbo vietų potinklį;	x	x
32.6.	testavimo potinklį.	x	x
33.	Mobiliuosiuose įrenginiuose ir kompiuterinėse darbo vietose turi būti naudojamos vykdomojo kodo (angl. <i>Executable code</i>) kontrolės priemonės, kuriomis apriojamas neleistino vykdomojo kodo naudojimas ar informuojamas administratorius apie neleistino vykdomojo kodo naudojimą.	x	x
34.	Turi būti parengti ir įdiegti kompiuterinių darbo vietų (įskaitant nešiojamuosius įrenginius) operacinių sistemų atvaizdai ir (arba) kitos priemonės su integruotomis saugumo nuostatomis. Atvaizde turi būti nustatyti tik veiklai būtini operacinių sistemų komponentai (administravimo paskyros, paslaugos (angl. <i>Services</i>), taikomosios programos, tinklo prievadai, atnaujinimai, sisteminės priemonės). Atvaizdai turi būti reguliariai peržiūrimi ir atnaujinami, iškart atnaujinami nustačius naujų spragų ar atakų. Pagal parengtus atvaizdus į kompiuterines darbo vietas (įskaitant nešiojamuosius įrenginius) turi būti įdiegiama operacinė sistema su saugumo nuostatomis.	x	x
35.	Draudžiama svetainės serveriuose saugoti sesijos duomenis (identifikatorių) prisijungimo tikslams, pasibaigus susijungimo sesijai.	x	x
36.	Internetu prieinamoms svetainėms, tinklų ir informacinėms sistemoms turi būti naudojama svetainės saugasienė (angl. <i>Web Application Firewall</i>).	x	x
37.	Internetu prieinamoms svetainėms, tinklų ir informacinėms sistemoms turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų remiantis OWASP (angl. <i>The Open Web Application Security Project</i>) Top 10 geriausiomis praktikomis (www.owasp.org).	x	x
38.	Žiniatinklio (angl. <i>Web</i>) formose turi būti naudojama	x	x

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
	svetainės naudotojo įvedamų duomenų kontrolė (angl. <i>Input validation</i>).		
39.	Internetu prieinamos tinklų ir informacinės sistemos neturi rodyti naudotojui klaidų pranešimų apie tinklų ir informacinės sistemos ir programinį kodą ar serverį.	x	x
40.	Internetu naudojant HTTPS protokolą (angl. <i>HyperText Transfer Protocol Secure</i> , HTTPS) prieinamos tinklų ir informacinės sistemos saugumo priemonės turi leisti tik jų funkcionalumui užtikrinti reikalingus protokolo metodus.	x	x
41.	Kibernetinio saugumo subjekto serveriuose ir kompiuterinėse darbo vietose turi būti naudojamos (jei įmanoma, centralizuotai) valdomos ir atnaujinamos kenkimo programinės įrangos aptikimo, stebėjimo realiu laiku priemonės.	x	x
42.	Naudojama tik legali ir leistina (pagal kibernetinio saugumo subjekto patvirtintą sąrašą) programinė įranga.	x	x
43.	Nuolatos turi būti stebimas tinklų ir informacinių sistemų įrangos laisvos atminties ar vietos diske kiekis, stebima apkrova, resursų naudojimas. Pasiekus nustatytas ribines reikšmes, apie tai turi būti informuojami atsakingi asmenys.	x	x

AŠTUNTASIS SKIRSNIS

KIBERNETINIO SAUGUMO REIKALAVIMŲ VEIKSMINGUMO VERTINIMAS

48. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi nustatyti kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarką, apimančią:

48.1. reikalavimą reguliariai, ne rečiau kaip kartą per metus, įvertinti kibernetinio saugumo subjekto atitiktį Kibernetinio saugumo įstatymui, šio Aprašo ir kibernetinio saugumo subjekto patvirtintiems kibernetinio saugumo politikos dokumentuose nustatytiems reikalavimams (toliau – Atitikties vertinimas).

48.2. kibernetinio saugumo subjektui atlikus Atitikties vertinimą, rengiami ir kibernetinio saugumo subjekto vadovo ar jo įgalioto asmens tvirtinami:

48.2.1. atitikties vertinimo ataskaita;

48.2.2. identifiкуotų neatitikčių (jei nustatyta) šalinimo planas, kuriame paskirti atsakingi vykdytojai, reikalingi ištekliai ir nustatyti įgyvendinimo terminai.

48.3. reikalavimą reguliariai, ne rečiau kaip kartą per 3 metus, atlikti kibernetinio saugumo auditą, vadovaujantis Kibernetinio saugumo įstatymo 14 straipsnio 8 punkto nuostatomis;

49. Kibernetinio saugumo subjektas, atsižvelgdamas į rizikų vertinimo rezultatus, įvykusių kibernetinio saugumo incidentus ir jų valdymo rezultatus, nustato kibernetinio saugumo taikomų priemonių veiksmingumo vertinimo reikalavimus:

49.1. kokias kibernetinio saugumo reikalavimų valdymo priemones reikia stebėti ir vertinti;

49.2. kokius stebėsenos, matavimo, analizės ir vertinimo metodus kibernetinio saugumo subjektas taiko;

49.3. kokių periodiškumą turi būti atliekama nustatytų metodų stebėsenos ir matavimai;

49.4. už veiksmingumo vertinimo stebėjimą ir matavimą atsakingus asmenis;

49.5. veiksmingumo vertinimo rezultatų analizės periodiškumą;

49.6. taikomų kibernetinių saugumo priemonių gerinimą, atsižvelgiant į vertinimo rezultatus.

50. NKSC, atlikdamas kibernetinio saugumo subjekto patikrinimą, turi teisę pareikalauti kibernetinio saugumo subjekto pateikti atliktų kibernetinio saugumo audito, atitikties vertinimo ataskaitos, atitikties vertinimo metu nustatytų neatitikčių šalinimo plano, rizikų vertinimo ataskaitos ir rizikų valdymo plano kopijas. Kibernetinio saugumo subjektas šiuos dokumentus turi pateikti į KSIS ne vėliau kaip per 5 darbo dienas nuo NKSC prašymo gavimo dienos.

51. Esminis kibernetinio saugumo subjektas ne rečiau kaip kartą per metus teikia atitikties kibernetinio saugumo reikalavimams vertinimą, užpildydamas NKSC klausimyną KSIS.

DEVINTASIS SKIRSNIS

KIBERNETINĖS HIGIENOS PRAKTIKA IR KIBERNETINIO SAUGUMO MOKYMAI

52. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi nustatyti kibernetinės higienos praktikos organizavimo ir kibernetinio saugumo mokymų organizavimo ir vykdymo tvarką. Kibernetinio saugumo vadovas turi užtikrinti, kad ne rečiau kaip kartą per metus visi kibernetinio saugumo subjekto darbuotojai išklaustyti kibernetinės higienos praktikos mokymus.

53. Kibernetinio saugumo subjektas turi užtikrinti darbuotojų informavimą apie kibernetinio saugumo aktualijas (mokymo ir informavimo būdai pasirenkami atsižvelgiant į tinklų ir informacinės sistemos specifiką).

54. Per tris mėnesius po kibernetinio saugumo klausimais organizuotų mokymų turi būti parengta mokymų ataskaita, kurioje turi būti nurodyta mokymų tema, dalyvių skaičius. Mokymus nurodytomis temomis kibernetinio saugumo subjektas turi teisę įsigyti iš trečiųjų šalių arba organizuoti pats. Kibernetinio saugumo subjektas parengtą mokymų ataskaitą turi saugoti ne mažiau kaip trejus metus nuo ataskaitos patvirtinimo datos.

DEŠIMTASIS SKIRSNIS

KRIPTOGRAFIJOS IR ŠIFRAVIMO NAUDOJIMO POLITIKA IR PROCEDŪROS

55. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi nustatyti kriptografijos ir šifravimo naudojimo tvarką, apimančią:

55.1. kibernetinio saugumo subjekto kriptografijos ir šifravimo priemonių naudojimo nuostatas, atsižvelgiant į kibernetinio saugumo subjekto nustatytus informacijos klasifikavimo ir tvarkymo reikalavimus;

55.2. raktų valdymą (generavimas, sunaikinimas, archyvavimas ir kt.).

56. Praradus kriptografinį raktą turi būti informuojamas atsakingas asmuo.

57. Kibernetinio saugumo subjektams taikomi techniniai reikalavimai nurodyti 4 lentelėje.

4 lentelė

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
44.	Viešaisiais elektroninių ryšių tinklais perduodamos kibernetinio saugumo subjektui jautrios informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą ar virtualųjį privatų tinklą (angl. <i>Virtual private network</i> , VPN).	x	x
45.	Belaidis ryšys turi būti šifruojamas pagal gerąją saugumo praktiką rekomenduojamu šifravimo ilgio raktu. Naudoti visuotinai saugiais pripažįstamus raktus ir protokolų versijas. Belaidės prieigos stotelėje turi būti pakeisti standartiniai gamintojo raktai.	x	x
46.	Duomenys, perduodami tarp mobiliojo įrenginio ir tinklų ir informacinės sistemos, turi būti šifruojami taikant virtualaus privataus tinklo (VPN) technologiją su TLS / SSL sertifikatu arba naudojama privataus prieigos taško (angl. <i>Access Point Name</i> , APN) per mobiliojo ryšio operatorių technologija, taikant perduodamų duomenų šifravimą sraute su TLS / SSL sertifikatu, kai VPN technologija nėra palaikoma mobiliųjų įrenginių.	x	x
47.	Mobiliųjų įrenginių laikmenose ir išorinėse kompiuterinėse laikmenose laikomi tinklų ir informacinių sistemų duomenys turi būti šifruojami.	x	x
48.	Turi būti įgyvendinti svetainės kriptografijos reikalavimai:		
48.1.	turi būti naudojami oficialiai pripažinti saugus ilgio	x	x

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
	raktai;		
48.2.	atliekant svetainės administravimo darbus, ryšys turi būti šifruojamas;	x	x
48.3.	šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų;	x	x
48.4.	turi būti naudojamas TLS standartas (1.3 versija arba naujesnė);	x	
48.5.	svetainės kriptografinės funkcijos turi būti įdiegtos serverio, kuriame yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. <i>Hardware security module</i>);	x	x
48.6.	visi kriptografiniai moduliai turi gebėti saugiai sutrikti (angl. <i>fail securely</i>).	x	
49.	Duomenys atsarginėse kopijose turi būti užšifruoti (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijų informacijai neteisėtai atkurti.	x	x
50.	Turi būti saugomi ir stebimi audito įrašai, susiję su kriptografinių raktų valdymo veikla (generavimas, sunaikinimas, archyvavimas, naudotojų veiksmai).	x	x

VIENUOLIKTASIS SKIRSNIS

ŽMOGIŠKŲJŲ IŠTEKLIŲ SAUGUMAS, FIZINĖS PRIEIGOS POLITIKA IR TURTO VALDYMAS

58. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi nustatyti žmogiškųjų išteklių saugumo reikalavimus, kurie apimtų:

58.1. reikalavimą, kad prieiga prie kibernetinio saugumo subjekto tinklų ir informacinės sistemos kibernetinio saugumo subjekto darbuotojams ir (arba) paslaugų teikėjams būtų suteikiama tik susipažinus su kibernetinio saugumo politikos dokumentais ir sutikus jų laikytis;

58.2. kibernetinio saugumo subjekto darbuotojų ir (arba) paslaugų teikėjų konfidencialumo arba informacijos neatskleidimo reikalavimus.

59. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi patvirtinti tinklų ir informacinių sistemų fizinės prieigos reikalavimus, apimančius:

59.1. patalpų, kurios turi būti apsaugotos (patalpos, kuriose laikoma kibernetinio saugumo subjekto tinklų ir informacinių sistemų įranga, serveriai, naudotojų ir administratorių darbo vietos), sąrašą;

59.2. saugomoms patalpoms taikomos fizinės aplinkos apsaugos ir prieigos kontrolės priemonės;

59.3. reikalavimą, kad į kibernetinio saugumo subjekto saugomas patalpas gali patekti tik įgalioti asmenys;

59.4. už fizinės apsaugos priemonių įgyvendinimą atsakingų asmenų paskyrimą.

60. Kibernetinio saugumo subjektams taikomi techniniai reikalavimai nurodyti 5 lentelėje.

5 lentelė

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams
51.	Tinklų ir informacinės sistemos serverių patalpos ir patalpos, kuriose saugomos atsarginės duomenų kopijos, turi būti apsaugotos nuo neteisėto asmenų patekimo į jas, taikant fizinės ar elektroninės apsaugos priemones.
52.	Kibernetinio saugumo subjekto nustatyta tvarka turi būti kontroliuojamas patekimas į tinklų ir informacinės sistemos serverių patalpas ir patalpas, kuriose saugomos atsarginės duomenų kopijos.

61. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi nustatyti kibernetinio saugumo subjekto turto valdymo tvarką, apimančią:

61.1. reikalavimą parengti ir nuolat atnaujinti tinklų ir informacinių sistemų turto (kibernetinio saugumo subjekto valdoma techninė ir programinė įranga, duomenys), kuriuo grindžiamos kibernetinio saugumo subjekto veiklos funkcijos, sąrašą (toliau – turto sąrašas);

61.2. turto klasifikavimo reikalavimus pagal jų svarbą, konfidencialumo, vientisumo ir prieinamumo atžvilgiu;

61.3. turto perkėlimo už kibernetinio saugumo subjekto ribų reikalavimus;

61.4. nešiojamųjų, keičiamųjų duomenų laikmenų naudojimo reikalavimus;

61.5. mobiliųjų įrenginių, kurie gali veikti savarankiškai ir turėti ryšį su tinklu ar internetu keičiantis jų buvimo vietai (pavyzdžiui, nešiojamasis kompiuteris, delninukas, išmanusis telefonas) ir naudojamų prisijungti prie kibernetinio saugumo subjektų tinklų ir informacinių sistemų, saugaus naudojimo ir kontrolės reikalavimus.

62. Tinklų ir informacinės sistemos įrangos priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai.

63. Tinklų ir informacinių sistemų techninės įrangos gedimai turi būti registruojami.

64. Kibernetinio saugumo subjektams taikomi techniniai reikalavimai nurodyti 6 lentelėje.

6 lentelė

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
53.	Naudojamos techninės priemonės, kurios apribotų neleistinų (turto sąraše nesančių) įrenginių prijungimą prie kibernetinio saugumo subjekto tinklų ir informacinių sistemų, apribotų neleistinos techninės įrangos naudojimą ir informuotų kibernetinio saugumo subjekto įgaliotą asmenį.	x	x
54.	Kibernetinio saugumo subjektas turi centralizuotai valdyti mobiliuosius įrenginius, kurie turi prieigą prie tinklų ir informacinių sistemų, ir juose įdiegtą programinę įrangą.	x	x
55.	Mobilieji įrenginiai, kuriais naršoma internete, turi būti apsaugoti nuo judriųjų programų (angl. <i>mobile code</i>) keliamų grėsmių.	x	
56.	Mobiliuosiuose įrenginiuose privalo būti įdiegtos priemonės, leisiančios nuotoliniu būdu neatkuriamai ištrinti mobiliuosiuose įrenginiuose esančius duomenis.	x	
57.	Reikalavimai tinklų ir informacinės sistemos techninei ir programinei įrangai ir patalpoms:		
57.1.	tinklų ir informacinių sistemų kompiuterinė įranga, kurią kibernetinio saugumo subjektas įvertino kaip svarbią, turi turėti įtampos filtrą ir nepertraukiamo maitinimo šaltinį, užtikrinantį techninės įrangos veikimą;	x	x
57.2.	jei tinklų ir informacinių sistemų serverių patalpose esančios įrangos bendras galingumas yra daugiau nei 10 kilovatų, turi būti įrengta oro kondicionavimo įranga;	x	x
57.3.	serverių patalpose turi būti oro kondicionavimo ir drėgmės kontrolės įranga;	x	
57.4.	tinklų ir informacinės sistemos techninė ir programinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;	x	x

57.5.	tinklų ir informacinės sistemos serverių patalpose turi būti įrengti gaisro ir įsilaužimo jutikliai, prijungti prie pastato signalizacijos ir (arba) apsaugos tarnybos stebėjimo pulto;	x	x
57.6.	visose patalpose, kuriose yra kibernetinio saugumo subjekto techninė įranga, turi būti įrengti gaisro jutikliai ir (ar) kitos fizinės apsaugos priemonės;	x	
57.7	kritiniai elementai (oro kondicionavimo įranga, vėdinimas ir drėgmės kontrolė, el. energijos tiekimas) turi būti dubliuojami, siekiant užtikrinti aukštą patalpoms eksploatuoti būtinų įrenginių patikimumą.	x	

DVYLIKTASIS SKIRSNIS

PRIEIGOS VALDYMAS IR KELIŲ VEIKSNIŲ TAPATUMO NUSTATYMO PRIEMONĖS

65. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi nustatyti prieigos valdymo tvarką, apimančią:

65.1. kibernetinio saugumo subjekto naudotojų, administratorių, paslaugų teikėjų grupių sudarymą, teisių ir prieigos prie kibernetinio saugumo subjekto tinklų ir informacinių sistemų suteikimą ir valdymą;

65.2. administratoriaus (administratorių) prieigos prie tinklų ir informacinės sistemos lygius ir juose taikomus kibernetinio saugumo reikalavimus (duomenų skaitymas, kūrimas, atnaujinimas, naikinimas, tinklų ir informacinės sistemos naudotojų informacijos, prieigos teisių redagavimas ir panašiai);

65.3. tinklų ir informacinių sistemų naudotojų registravimo ir išregistravimo reikalavimus ir už šių veiksmų atlikimą atsakingo asmens paskyrimą;

65.4. priemonės tinklų ir informacinių sistemų naudotojų tapatybei nustatyti;

65.5. tinklų ir informacinės sistemos naudotojų ir administratorių slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimus:

65.5.1. reikalavimą, kad slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir panašiai);

65.5.2. reikalavimą, kad slaptažodis negali būti sudarytas iš pasikartojančių arba nuoseklių simbolių (pvz., „aaaaaaaaaaaa“ arba „0123456789“) ar įprastos klaviatūros sekos (pvz., „Qwerty“);

65.5.3. draudimą techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti vadovaujantis šiame skyriuje nustatytais reikalavimais;

65.6. draudimą slaptažodžius atskleisti kitiems asmenims;

65.7. sąlygas ir atvejus, kada panaikinama tinklų ir informacinės sistemos naudotojų ir administratorių teisė dirbti su konkrečia informacija;

65.8. leistinus nuotolinio naudotojų ir administratorių prisijungimo prie tinklų ir informacinės sistemos būdus;

65.9. kelių veiksmų tapatumo priemonių naudojimo būdus.

66. Kibernetinio saugumo subjektas turi patvirtinti asmenų, kuriems suteiktos administratoriaus teisės prisijungti prie tinklų ir informacinių sistemų, sąrašą, kuris periodiškai turi būti peržiūrimas už kibernetinį saugumą atsakingo asmens. Sąrašas turi būti peržiūrėtas, kai administratorius nušalinamas arba pasibaigia jo darbo (tarnybos) santykiai.

67. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jeigu naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

68. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo turi patvirtinti kelių veiksmų tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimo nuostatas.

69. Kibernetinio saugumo subjektams taikomi techniniai reikalavimai nurodyti 7 lentelėje.

7 lentelė

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
58.	Administratoriaus funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms naudotojo funkcijoms atlikti.	x	x
59.	Naudotojams negali būti suteikiamos administratoriaus teisės.	x	x
60.	Kiekvienas naudotojas turi būti unikaliai atpažįstamas.	x	x
61.	Naudotojas ir administratorius turi patvirtinti savo tapatybę slaptažodžiu ir papildoma tapatumo nustatymo priemone (kelių veiksmų tapatumo nustatymo priemonės).	x	x
62.	Naudotojo teisė dirbti su konkrečia tinklų ir informacine sistema turi būti sustabdoma, kai naudotojas nesinaudoja tinklų ir informacine sistema ilgiau kaip 3 mėnesius.	x	x
63.	Administratoriaus teisė dirbti su tinklų ir informacine	x	x

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
	sistema turi būti sustabdoma, kai administratorius nesinaudoja tinklų ir informacine sistema ilgiau kaip 2 mėnesius.		
64.	Kai naudotojas ar administratorius nušalinamas nuo darbo (pareigų), neatitinka kituose teisės aktuose nustatytų naudotojo ar administratoriaus kvalifikacinių reikalavimų, taip pat pasibaigia jo darbo (tarnybos) santykiai, jis praranda patikimumą, jo teisė naudotis tinklų ir informacine sistema turi būti panaikinta nedelsiant, bet ne vėliau kaip per kibernetinio saugumo subjekto nustatytą terminą.	x	x
65.	Nereikalingos ar nenaudojamos tinklų ir informacinių sistemų paskyros turi būti blokuojamos nedelsiant, bet ne vėliau kaip per kibernetinio saugumo subjekto nustatytą terminą ir ištrinamos praėjus žurnalinių įrašų saugojimo terminui (ne trumpiau kaip 90 kalendorinių dienų).	x	x
66.	Baigus darbą arba pasitraukiant iš darbo vietos, turi būti atsijungiama nuo tinklų ir informacinių sistemų, įjungiama ekrano užsklanda su slaptažodžiu.	x	x
67.	Tinkluose ir informacinėse sistemose neatliekant jokių veiksmų, darbo stotis turi užsirakinti (ne ilgiau nei po 15 minučių), kad toliau naudotis tinklų ir informacine sistema būtų galima tik pakartotinai patvirtinus savo tapatybę.	x	x
68.	Tinklų ir informacinės sistemos dalys, tarp jų ir svetainės ir naršyklės, patvirtinančios naudotojo tapatumą, turi drausti išsaugoti slaptažodžius, išskyrus specializuotą slaptažodžių tvarkymo programinę įrangą.	x	x
69.	Slaptažodis turi būti sudarytas iš didžiųjų ir mažųjų raidžių, skaičių ir specialiųjų simbolių.	x	x
70.	Turi būti nustatytas maksimalus leistinas naudotojų mėginimų prisijungti prie tinklų ir informacinių sistemų skaičius – ne daugiau negu 5 kartai iš eilės. Po numatyto	x	x

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
	bandymų skaičiaus prisijungti prie tinklų ir informacinių sistemų paskyra turi užsiblokuoti. Atblokuoti gali tik įgalioti asmenys.		
71.	Papildomi naudotojo slaptažodžių reikalavimai:		
71.1.	slaptažodis turi būti keičiamas ne rečiau kaip kas 6 mėnesius;	x	x
71.2.	slaptažodį turi sudaryti ne mažiau kaip 10 simbolių;	x	x
71.3.	keičiamo slaptažodžio neturi būti leidžiama sudaryti iš buvusių 6 paskutinių slaptažodžių;	x	x
71.4.	pirmąkart jungiantis prie tinklų ir informacinių sistemų, turi būti reikalaujama, kad naudotojas pakeistų slaptažodį;	x	x
71.5.	naudotojas turi turėti galimybę bet kuriuo metu pasikeisti slaptažodį.	x	x
72.	Papildomi administratorių slaptažodžių reikalavimai:		
72.1.	slaptažodis turi būti keičiamas ne rečiau kaip kas 6 mėnesius;	x	x
72.2.	slaptažodį turi sudaryti ne mažiau kaip 15 simbolių;	x	x
72.3.	keičiant slaptažodį, neturi būti leidžiama naudoti slaptažodžio iš buvusių 8 paskutinių slaptažodžių.	x	x
73.	Turi būti vykdoma administratorių paskyrų kontrolė:		
73.1.	reguliariai, ne rečiau kaip kartą per metus, tikrinama, ar administratoriaus paskyros atitinka šiame skyriuje nustatytus reikalavimus, ir pranešama įgaliotam atsakingam asmeniui apie administratorių paskyras, kurios neatitinka šiame skirsnyje nustatytų reikalavimų;		x
73.2.	naudojamos administratorių paskyrų kontrolės priemonės, kurios periodiškai tikrina administratoriaus paskyras. Apie administratoriaus paskyras, kurios neatitinka šiame skirsnyje nustatytų reikalavimų, turi	x	

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams	Esminiams	Svarbiems
	būti pranešama įgaliotam asmeniui.		
74.	Vykdoma naudotojų paskyrų kontrolė:		
74.1.	reguliariai tikrinama, ar naudotojų paskyros atitinka šiame skirsnyje nustatytus reikalavimus. Apie naudotojų paskyras, kurios neatitinka šiame skirsnyje nustatytų reikalavimų, turi būti pranešama įgaliotam asmeniui;		x
74.2.	naudojamos naudotojų paskyrų kontrolės priemonės, kurios periodiškai tikrina naudotojų paskyras. Apie naudotojų paskyras, kurios neatitinka šiame skirsnyje nustatytų reikalavimų, turi būti pranešama įgaliotam asmeniui.	x	
75.	Lokalių naudotojų ir administratorių paskyros turi atitikti reikalavimus, nurodytus šiame skirsnyje.	x	x
76.	Papildomi atpažinties, tapatumo patvirtinimo ir naudojimosi kontrolės reikalavimai (kibernetinio saugumo subjekto svetainėms, pasiekiamoms iš viešųjų elektroninių ryšių tinklų):		
76.1.	programiniame kode draudžiama išsaugoti duomenis (vardą, slaptažodį, aplikacijų programavimo sąsajas (angl. <i>Application programming interface</i>) raktus / ženklus (angl. <i>Token</i>) ir kt.), kuriuos atskleidus gali būti pasinaudota prieiga prie įrenginių, resursų, paskyrų ar valdiklių.	x	x

III SKYRIUS

BAIGIAMOSIOS NUOSTATOS

70. Aprašo reikalavimų įgyvendinimas kibernetinio saugumo subjektų neatleidžia nuo pareigos įgyvendinti ir kituose teisės aktuose nustatytų reikalavimų, kuriais siekiama užtikrinti tinklų ir informacinių sistemų saugumą, išskyrus Kibernetinio saugumo įstatymo 1 straipsnio 3 dalyje numatytus atvejus.

71. Kibernetinio saugumo subjektai kibernetinio saugumo reikalavimus privalo įgyvendinti ne vėliau kaip per 12 mėnesių nuo jų įregistravimo Kibernetinio saugumo informacinėje sistemoje dienos, išskyrus Aprašo 72 punkte numatytus atvejus.

72. Kibernetinio saugumo subjektai techninius kibernetinio saugumo reikalavimus, nustatytus Aprašo 26, 31, 47, 57, 60, 64, 69 punktuose, privalo įgyvendinti ne vėliau kaip per 24 mėnesius nuo jų įregistravimo Kibernetinio saugumo informacinėje sistemoje dienos.

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2018 m. rugpjūčio 13 d. nutarimu Nr. 818
(Lietuvos Respublikos Vyriausybės
2024 m. lapkričio 6 d. nutarimo Nr. 945
redakcija)

VYKDYMO UŽTIKRINIMO PRIEMONIŲ TAIKymo KIBERNETINIO SAUGUMO SUBJEKTAMS TVARKOS APRAŠAS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Vykdymo užtikrinimo priemonių taikymo kibernetinio saugumo subjektams tvarkos aprašas (toliau – Aprašas) reglamentuoja vykdymo užtikrinimo priemonių parinkimą, vykdymo užtikrinimo priemonių taikymą esant keletui pažeidimų ir baudų kibernetinio saugumo subjektams skyrimą.

2. Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme.

II SKYRIUS VYKDYMO UŽTIKRINIMO PRIEMONIŲ PARINKIMAS

3. Vykdymo užtikrinimo priemonės parinkimas susideda iš:

3.1. Kibernetinio saugumo įstatymo 28 straipsnio 3–5 dalyse nurodytų aplinkybių vertinimo. Vertinant Kibernetinio 28 straipsnio 3 dalies 2–9 punktuose nurodytas aplinkybes atsižvelgiama į šių aplinkybių teigiamus ir neigiamus aspektus Aprašo 4 punkte nustatyta tvarka;

3.2. Vykdymo užtikrinimo priemonės (-ių) parinkimo, atsižvelgiant į vykdymo užtikrinimo priemonės taikymo tikslingumą.

4. Kibernetinio saugumo įstatymo 28 straipsnio 3 dalies 2–9 punktuose nurodytų aplinkybių vertinimas atliekamas identifikuojant šių aplinkybių teigiamus ir neigiamus aspektus:

4.1. Kibernetinio saugumo įstatymo 28 straipsnio 3 dalies 2 punkte nurodytos aplinkybės vertinimas:

4.1.1. Teigiamai vertinama, jei pažeidimų trukmė buvo sumažinta dėl optimalių bei nekeliančių rizikų kibernetinio saugumo subjekto veiksmų.

4.1.2. Neigiamai vertinami pažeidimai, dėl kurių trukmės kyla didesnės žalos ir neigiamo poveikio atsiradimo grėsmė, apsunkinamas žalos ar neigiamo poveikio panaikinimas, trikdomas Nacionalinio kibernetinio saugumo centro gebėjimas tinkamai reaguoti į pažeidimą.

4.2. Kibernetinio saugumo įstatymo 28 straipsnio 3 dalies 3 punkte nurodytos aplinkybės vertinimas:

4.2.1. Teigiamai vertinama, jei pažeidimų pastaruosius dvejus metus nebuvo.

4.2.2. Neigiamai vertinami kibernetinio saugumo subjekto per pastaruosius dvejus metus įvykdyti pažeidimai. Kuo ilgesnis laikotarpis nuo ankstesnio pažeidimo iki šiuo metu tiriamo pažeidimo, tuo mažesnė šios aplinkybės svarba skiriant vykdymo užtikrinimo priemonę.

4.3. Kibernetinio saugumo įstatymo 28 straipsnio 3 dalies 4 punkte nurodytos aplinkybės vertinimas:

4.3.1. Teigiamai vertinama, kai nuostoliai atlyginti ar padarytas neigiamas poveikis panaikintas kibernetinio saugumo subjekto iniciatyva.

4.3.2. Neigiamai vertinama nuostolių neatlyginimas ar padaryto neigiamo poveikio nepanaikininimas.

4.4. Kibernetinio saugumo įstatymo 28 straipsnio 3 dalies 5 punkte nurodytos aplinkybės vertinimas:

4.4.1. Teigiamai vertinamas kibernetinio saugumo priemonių įdiegimas prieš Nacionaliniam kibernetinio saugumo centrui pradedant patikrinimą ir kibernetinio saugumo subjektui apie jį sužinant, taip pat kibernetinio saugumo priemonių, kurias pasitelkiant pavyko užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti, buvimas, taip pat šių priemonių pritaikymas laiku.

4.4.2. Neigiamai vertinama, kai kibernetinio saugumo subjektas nesiima priemonių užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti.

4.5. Kibernetinio saugumo įstatymo 28 straipsnio 3 dalies 6 punkte nurodytos aplinkybės vertinimas:

4.5.1. Teigiamai vertinama, jei kibernetinio saugumo subjektas apie pažeidimą laiku ir tinkamu būdu informavo subjektus, kurie pagal nustatytus elgesio kodeksus arba patvirtintus sertifikavimo mechanizmus turėjo gauti tokią informaciją.

4.5.2. Neigiamai vertinama, kai kibernetinio saugumo subjektas nesilaikė elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų ir tai tiesiogiai susiję su pažeidimu.

4.6. Kibernetinio saugumo įstatymo 28 straipsnio 3 dalies 7 punkte nurodytos aplinkybės vertinimas:

4.6.1. Teigiamai vertinama, kai kibernetinio saugumo subjektas reagavo į Nacionalinio kibernetinio saugumo centro reikalavimus patikrinimo metu ir todėl patikrinimas vyko greičiau ir efektyviau, taip pat teigiamai vertinama, kai kibernetinio saugumo subjektas pripažino pažeidimą, savo iniciatyva pranešė apie pažeidimą prieš tai, kai Nacionalinis kibernetinio saugumo centras apie jį sužinojo.

4.6.2. Neigiamai vertinama, kai dėl kibernetinio saugumo subjekto sisteminių ir pasikartojančių veiksmų patikrinimas ar kiti priežiūros veiksmai užtruko.

4.7. Kibernetinio saugumo įstatymo 28 straipsnio 3 dalies 8 punkte nurodytos aplinkybės vertinimas:

4.7.1. Teigiamai vertinama, kai nurodytų pažeidimų mastas buvo sumažintas dėl optimalių ir nekeliančių rizikų kibernetinio saugumo subjekto veiksmų.

4.7.2. Neigiamai vertinama, kai pažeidimas sudaro sąlygas paveikti gyvybiškai svarbių paslaugų teikimą, taip pat kai pažeidimas yra susijęs su esminių kibernetinio saugumo subjektų valdomomis ir tvarkomomis tinklų informacinėmis sistemomis.

4.8. Kibernetinio saugumo įstatymo 28 straipsnio 3 dalies 9 punkte nurodytos aplinkybės vertinimas:

4.8.1. Neutraliu veiksmu laikoma, kai pažeidimas padarytas dėl neatsargumo.

4.8.2. Neigiamai vertinami tyčiniai pažeidimai.

5. Vykdyto užtikrinimo priemonė (-ės), įvertinus Kibernetinio saugumo įstatymo 28 straipsnio 3–5 dalyse nurodytas aplinkybes, parenkama (-os) atsižvelgiant į vykdyto užtikrinimo priemonės (-ių) taikymo tikslumą:

5.1. Jei įvertinus Kibernetinio saugumo įstatymo pažeidimą (toliau – pažeidimas) ir jo aplinkybes nustatoma, kad Kibernetinio saugumo įstatymo reikalavimams įgyvendinti netikslinga skirti vykdyto užtikrinimo priemonių, nurodančių konkrečias taikytinas priemones ar apribojančių kibernetinio saugumo subjektų veiklą, taikomos viena ar kelios vykdyto užtikrinimo priemonės iš nurodytų Kibernetinio saugumo įstatymo 28 straipsnio 1 dalies 1 ir (ar) 3 punktuose.

5.2. Jei įvertinus pažeidimą ir jo aplinkybes nustatoma, kad Kibernetinio saugumo įstatymo reikalavimams įgyvendinti tikslinga skirti pažeidimą ir (ar) jo atsiradimo veiksmus ir priežastis šalinančių vykdyto užtikrinimo priemonių, taikomos viena ar kelios vykdyto užtikrinimo priemonės iš nurodytų Kibernetinio saugumo įstatymo 28 straipsnio 1 dalies 2, 4, 6 ir (ar) 7 punktuose.

5.3. Jei įvertinus pažeidimą ir jo aplinkybes nustatoma, kad apie pažeidimą tikslinga informuoti visuomenę ar tam tikras visuomenės grupes, taikomos viena ar kelios vykdyto užtikrinimo priemonės iš nurodytų Kibernetinio saugumo įstatymo 28 straipsnio 1 dalies 5 ir (ar) 8 punktuose.

5.4. Jei įvertinus pažeidimą ir jo aplinkybes nustatoma, kad Kibernetinio saugumo įstatymo 28 straipsnio 1 dalies 1–8 ir (ar) 10, 11 papunkčiuose nurodyta vykdyto užtikrinimo priemonė pažeidimą padariusiam kibernetinio saugumo subjektui neturės atgrasomojo poveikio arba atgrasomasis poveikis bus nepakankamas, kartu su Kibernetinio saugumo įstatymo 28 straipsnio 1 dalies 1–8 ir (ar) 10, 11 papunkčiuose nurodyta (-omis) vykdyto užtikrinimo priemone (-ėmis) taikoma ir Kibernetinio saugumo įstatymo 28 straipsnio 1 dalies 9 punkte numatyta vykdyto užtikrinimo priemonė. Vertinant atgrasomąjį poveikį įvertinama, ar kibernetinio saugumo subjekto patiriama nauda tęsiant pažeidimą nėra didesnė už vykdyto užtikrinimo priemonės sukeltą poveikį ir ar kibernetinio saugumo subjektui už ankstesnius pažeidimus skirtų vykdyto užtikrinimo priemonių taikymas leido pasiekti teigiamų tikslų.

III SKYRIUS

VYKDYMO UŽTIKRINIMO PRIEMONIŲ TAIKYMAS ESANT KELETUI PAŽEIDIMŲ

6. Jeigu atlikus patikrinimą nustatoma keletas pažeidimų, vykdyto užtikrinimo priemonės taikomos šiuo būdu:

6.1. Kai yra keli pažeidimai, kilę dėl atskirų veiksmų ar neveikimo, vykdymo užtikrinimo priemonės taikomos atskirai už kiekvieną pažeidimą.

6.2. Kai yra keli pažeidimai, kilę dėl vieno veiksmo ar neveikimo, vykdymo užtikrinimo priemonės taikomos atskirai, jei teisės aktų nuostatų taikymas už vieną pažeidimą neužkerta kelio kitų teisės aktų nuostatų taikomumui arba jų neapima.

6.3. Kai yra keli pažeidimai, kilę dėl vieno veiksmo ar neveikimo, poveikio vykdymo užtikrinimo priemonė taikoma už pavojingesnį, kaip suprantama pagal Kibernetinio saugumo įstatymo 29 straipsnį, pažeidimą, jei teisės aktų nuostatų taikymas dėl vieno pažeidimo užkerta kelią kitų teisės aktų nuostatų taikomumui arba jas apima.

IV SKYRIUS

BAUDŲ KIBERNETINIO SAUGUMO SUBJEKTAMS SKYRIMAS

7. Viena iš vykdymo užtikrinimo priemonių parinkus baudą, baudos skyrimo klausimas svarstomas ir sprendimas dėl baudos skyrimo priimamas Kibernetinio saugumo įstatymo 31 straipsnyje nustatyta tvarka.

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2018 m. rugpjūčio 13 d. nutarimu Nr. 818
(Lietuvos Respublikos Vyriausybės
2024 m. lapkričio 6 d. nutarimo Nr. 945
redakcija)

SAUGIOJO VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO NAUDOTOJŲ SĄRAŠAS

Eil. Nr.	Juridinio asmens pavadinimas
Lietuvos Respublikos aplinkos ministro valdymo sritis	
1.	Lietuvos Respublikos aplinkos ministerija
2.	Aplinkos apsaugos agentūra
3.	Lietuvos geologijos tarnyba prie Aplinkos ministerijos
4.	Lietuvos hidrometeorologijos tarnyba prie Aplinkos ministerijos
5.	Valstybinė teritorijų planavimo ir statybos inspekcija prie Aplinkos ministerijos
6.	Aplinkos apsaugos departamentas prie Aplinkos ministerijos
7.	Valstybinė miškų tarnyba
8.	Nacionalinė žemės tarnyba prie Aplinkos ministerijos
9.	Aplinkos ministerijos Aplinkos projektų valdymo agentūra
10.	Viešoji įstaiga Statybos sektoriaus vystymo agentūra
Lietuvos Respublikos energetikos ministro valdymo sritis	
11.	Lietuvos Respublikos energetikos ministerija
12.	Valstybės įmonė Ignalinos atominė elektrinė
13.	Viešoji įstaiga Lietuvos energetikos agentūra
14.	Valstybinė energetikos reguliavimo taryba
Lietuvos Respublikos finansų ministro valdymo sritis	
15.	Lietuvos Respublikos finansų ministerija

Eil. Nr.	Juridinio asmens pavadinimas
16.	Valstybės įmonė Turto bankas
17.	Audito, apskaitos, turto vertinimo ir nemokumo valdymo tarnyba prie Finansų ministerijos
18.	Valstybės duomenų agentūra
19.	Lošimų priežiūros tarnyba prie Finansų ministerijos
20.	Muitinės departamentas prie Finansų ministerijos
21.	Kauno teritorinė muitinė
22.	Klaipėdos teritorinė muitinė
23.	Muitinės informacinių sistemų centras
24.	Muitinės kriminalinė tarnyba
25.	Muitinės laboratorija
26.	Muitinės mokymo centras
27.	Vilniaus teritorinė muitinė
28.	Nacionalinis bendrųjų funkcijų centras
29.	Valstybės dokumentų technologinės apsaugos tarnyba prie Finansų ministerijos
30.	Valstybinė mokesčių inspekcija prie Finansų ministerijos
31.	Kauno apskrities valstybinė mokesčių inspekcija
32.	Klaipėdos apskrities valstybinė mokesčių inspekcija
33.	Panevėžio apskrities valstybinė mokesčių inspekcija
34.	Šiaulių apskrities valstybinė mokesčių inspekcija
35.	Vilniaus apskrities valstybinė mokesčių inspekcija
Lietuvos Respublikos krašto apsaugos ministro valdymo sritis	
36.	Lietuvos Respublikos krašto apsaugos ministerija
37.	Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos
38.	Centralizuota finansų ir turto tarnyba prie Krašto apsaugos ministerijos
39.	Generolo Jono Žemaičio Lietuvos karo akademija
40.	Gynybos resursų agentūra prie Krašto apsaugos ministerijos
41.	Infrastruktūros valdymo agentūra

Eil. Nr.	Juridinio asmens pavadinimas
42.	Krašto apsaugos ministerijos bendrųjų reikalų departamentas
43.	Lietuvos kariuomenė
44.	Mobilizacijos ir pilietinio pasipriešinimo departamentas prie Krašto apsaugos ministerijos
45.	Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos
46.	Vytauto Didžiojo karo muziejus
Lietuvos Respublikos kultūros ministro valdymo sritis	
47.	Lietuvos Respublikos kultūros ministerija
48.	Kultūros paveldo departamentas prie Kultūros ministerijos
49.	Lietuvos nacionalinis dailės muziejus
50.	Lietuvos nacionalinė Martyno Mažvydo biblioteka
51.	Viešoji įstaiga Lietuvos nacionalinis radijas ir televizija
Lietuvos Respublikos socialinės apsaugos ir darbo ministro valdymo sritis	
52.	Lietuvos Respublikos socialinės apsaugos ir darbo ministerija
53.	Jaunimo reikalų agentūra
54.	Pabėgėlių priėmimo centras
55.	Užimtumo tarnyba prie Socialinės apsaugos ir darbo ministerijos
56.	Lietuvos Respublikos valstybinė darbo inspekcija prie Socialinės apsaugos ir darbo ministerijos
57.	Asmens su negalia teisių apsaugos agentūra prie Socialinės apsaugos ir darbo ministerijos
58.	Socialinių paslaugų priežiūros departamentas prie Socialinės apsaugos ir darbo ministerijos
59.	Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba prie Socialinės apsaugos ir darbo ministerijos
60.	Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos
61.	Valstybinio socialinio draudimo fondo valdybos Kauno skyrius
62.	Valstybinio socialinio draudimo fondo valdybos Klaipėdos skyrius
63.	Valstybinio socialinio draudimo fondo valdybos Panevėžio skyrius
64.	Valstybinio socialinio draudimo fondo valdybos Vilniaus skyrius
65.	Techninės pagalbos priemonių centras
66.	Adakavo socialinių paslaugų namai
67.	Aknystos socialinės globos namai

Eil. Nr.	Juridinio asmens pavadinimas
68.	Dūseikių socialinės globos namai
69.	Ilguvos socialinės globos namai
70.	Jurdaičių socialinės globos namai
71.	Jotainių socialinės globos namai
72.	Jasiuliškių socialinės globos namai
73.	Kėdainių socialinės globos namai
74.	Kupiškio socialinės globos namai
75.	Lavėnų socialinės globos namai
76.	Linkuvos socialinės globos namai
77.	Macikų socialinės globos namai
78.	Marijampolės specialieji socialinės globos namai
79.	Prūdiškių socialinės globos namai
80.	Nijolės Genytės socialinės globos namai
81.	Padvarių socialinės globos namai
82.	Suvalkijos socialinės globos namai
83.	Strėvininkų socialinės globos namai
84.	Skemų socialinės globos namai
85.	Strūnos socialinės globos namai
86.	Stonaičių socialinės globos namai
87.	Specialieji socialinės globos namai „Tremtinių namai“
88.	Utenos socialinės globos namai
89.	Veisiejų socialinės globos namai
90.	Socialinės globos centras „Vija“
91.	Ventos socialinės globos namai
92.	Visagino socialinės globos namai
93.	Zarasų socialinės globos namai
94.	Algimanto Bandzos socialinių paslaugų namai

Eil. Nr.	Juridinio asmens pavadinimas
95.	Globos namai „Užuovėja“
Lietuvos Respublikos susisiekimo ministro valdymo sritis	
96.	Lietuvos Respublikos susisiekimo ministerija
97.	Akcinė bendrovė „Via Lietuva“
98.	Lietuvos transporto saugos administracija
99.	Pasienio kontrolės punktų direkcija prie Susisiekimo ministerijos
100.	Viešoji įstaiga „Plačiajuostis internetas“
Lietuvos Respublikos sveikatos apsaugos ministro valdymo sritis	
101.	Lietuvos Respublikos sveikatos apsaugos ministerija
102.	Higienos institutas
103.	Lietuvos sveikatos mokslų universiteto ligoninė Kauno klinikos
104.	Nacionalinė visuomenės sveikatos priežiūros laboratorija
105.	Nacionalinis transplantacijos biuras prie Sveikatos apsaugos ministerijos
106.	Radiacinės saugos centras
107.	Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centras
108.	Valstybinė teismo medicinos tarnyba
109.	Valstybinė teismo psichiatrijos tarnyba prie Sveikatos apsaugos ministerijos
110.	Valstybinė vaistų kontrolės tarnyba prie Sveikatos apsaugos ministerijos
111.	Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos

Eil. Nr.	Juridinio asmens pavadinimas
112.	Kauno teritorinė ligonių kasa
113.	Klaipėdos teritorinė ligonių kasa
114.	Panevėžio teritorinė ligonių kasa
115.	Šiaulių teritorinė ligonių kasa
116.	Vilniaus teritorinė ligonių kasa
117.	Greitosios medicinos pagalbos tarnyba
118.	Viešoji įstaiga Alytaus apskrities tuberkuliozės ligoninė
119.	Lietuvos sveikatos mokslų universiteto Kauno ligoninė
120.	Viešoji įstaiga Nacionalinis kraujo centras
121.	Viešoji įstaiga Klaipėdos universiteto ligoninė
122.	Viešoji įstaiga Respublikinė Klaipėdos ligoninė
123.	Viešoji įstaiga Respublikinė Panevėžio ligoninė
124.	Viešoji įstaiga Respublikinė Šiaulių ligoninė
125.	Viešoji įstaiga Respublikinė Vilniaus psichiatrijos ligoninė
126.	Viešoji įstaiga Respublikinė Vilniaus universitetinė ligoninė
127.	Viešoji įstaiga Rokiškio psichiatrijos ligoninė

Eil. Nr.	Juridinio asmens pavadinimas
128.	Viešoji įstaiga Vilniaus gimdymo namai
129.	Viešoji įstaiga Vilniaus universiteto ligoninė Santaros klinikos
130.	Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos
131.	Respublikinis priklausomybės ligų centras
132.	Valstybinė akreditavimo sveikatos priežiūros veiklai tarnyba prie Sveikatos apsaugos ministerijos
133.	Viešoji įstaiga Palangos vaikų rehabilitacijos sanatorija „Palangos gintaras“
Lietuvos Respublikos švietimo, mokslo ir sporto ministro valdymo sritis	
134.	Lietuvos Respublikos švietimo, mokslo ir sporto ministerija
135.	Nacionalinė švietimo agentūra
136.	Nacionalinis vėžio institutas
Lietuvos Respublikos teisingumo ministro valdymo sritis	
137.	Lietuvos Respublikos teisingumo ministerija
138.	Lietuvos kalėjų tarnyba
139.	Lietuvos probacijos tarnyba
140.	Lietuvos teismo ekspertizės centras
141.	Valstybinė duomenų apsaugos inspekcija
142.	Valstybinė vartotojų teisių apsaugos tarnyba

Eil. Nr.	Juridinio asmens pavadinimas
143.	Valstybės garantuojamos teisinės pagalbos tarnyba
144.	Lietuvos Respublikos valstybinis patentų biuras
Lietuvos Respublikos ekonomikos ir inovacijų ministro valdymo sritis	
145.	Lietuvos Respublikos ekonomikos ir inovacijų ministerija
146.	Lietuvos standartizacijos departamentas
147.	Valstybės skaitmeninių sprendimų agentūra
148.	Lietuvos metrologijos inspekcija
149.	Valstybės įmonė Registrų centras
150.	Viešoji įstaiga CPO LT
Lietuvos Respublikos užsienio reikalų ministro valdymo sritis	
151.	Lietuvos Respublikos užsienio reikalų ministerija (įskaitant Lietuvos Respublikos diplomatinės atstovybės ir konsulines įstaigas)
Lietuvos Respublikos vidaus reikalų ministro valdymo sritis	
152.	Lietuvos Respublikos vidaus reikalų ministerija
153.	Akcinė bendrovė „Regitra“
154.	Asmens dokumentų išrašymo centras prie Vidaus reikalų ministerijos
155.	Finansinių nusikaltimų tyrimo tarnyba prie Vidaus reikalų ministerijos
156.	Informatikos ir ryšių departamentas prie Vidaus reikalų ministerijos

Eil. Nr.	Juridinio asmens pavadinimas
157.	Vidaus reikalų ministerijos Medicinos centras
158.	Migracijos departamentas prie Vidaus reikalų ministerijos
159.	Policijos departamentas prie Vidaus reikalų ministerijos
160.	Alytaus apskrities vyriausiasis policijos komisariatas
161.	Kauno apskrities vyriausiasis policijos komisariatas
162.	Klaipėdos apskrities vyriausiasis policijos komisariatas
163.	Lietuvos kriminalinės policijos biuras
164.	Lietuvos policijos mokykla
165.	Marijampolės apskrities vyriausiasis policijos komisariatas
166.	Panevėžio apskrities vyriausiasis policijos komisariatas
167.	Šiaulių apskrities vyriausiasis policijos komisariatas
168.	Tauragės apskrities vyriausiasis policijos komisariatas
169.	Telšių apskrities vyriausiasis policijos komisariatas
170.	Utenos apskrities vyriausiasis policijos komisariatas
171.	Vilniaus apskrities vyriausiasis policijos komisariatas

Eil. Nr.	Juridinio asmens pavadinimas
172.	Išteklių agentūra prie Vidaus reikalų ministerijos
173.	Valstybės sienos apsaugos tarnyba prie Vidaus reikalų ministerijos
174.	Viešojo saugumo tarnyba prie Vidaus reikalų ministerijos
175.	Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Vidaus reikalų ministerijos
176.	Bendrasis pagalbos centras
177.	Gaisrinių tyrimų centras
178.	Ugniagesių gelbėtojų mokykla
Lietuvos Respublikos žemės ūkio ministro valdymo sritis	
179.	Lietuvos Respublikos žemės ūkio ministerija
180.	Valstybės įmonė Žemės ūkio duomenų centras
181.	Nacionalinė mokėjimo agentūra prie Žemės ūkio ministerijos
182.	Žuvininkystės tarnyba prie Žemės ūkio ministerijos
183.	Žemės ūkio agentūra prie Žemės ūkio ministerijos
184.	Valstybinė augalininkystės tarnyba prie Žemės ūkio ministerijos
185.	Nacionalinis maisto ir veterinarijos rizikos vertinimo institutas
Kita	
186.	Lietuvos Respublikos Prezidento kanceliarija

Eil. Nr.	Juridinio asmens pavadinimas
187.	Lietuvos Respublikos Seimo kanceliarija
188.	Lietuvos Respublikos Seimo kontrolierių įstaiga
189.	Lietuvos Respublikos Vyriausybės kanceliarija
190.	Vyriausybės strateginės analizės centras
191.	Vyriausybės atstovų įstaiga
192.	Lietuvos Respublikos valstybės saugumo departamentas
193.	Viešojo valdymo agentūra
194.	Lietuvos Respublikos valstybės kontrolė
195.	Narkotikų, tabako ir alkoholio kontrolės departamentas
196.	Lietuvos vyriausiojo archyvaro tarnyba
197.	Kauno regioninis valstybės archyvas
198.	Klaipėdos regioninis valstybės archyvas
199.	Lietuvos centrinis valstybės archyvas
200.	Lietuvos ypatingasis archyvas
201.	Lietuvos literatūros ir meno archyvas

Eil. Nr.	Juridinio asmens pavadinimas
202.	Lietuvos valstybės istorijos archyvas
203.	Lietuvos valstybės naujasis archyvas
204.	Šiaulių regioninis valstybės archyvas
205.	Vilniaus regioninis valstybės archyvas
206.	Lietuvių kalbos institutas
207.	Lietuvos Respublikos generalinė prokuratūra
208.	Nacionalinė teismų administracija
209.	Nacionalinės teismų administracijos mokymo centras
210.	Lietuvos bankas
211.	Valstybinė maisto ir veterinarijos tarnyba
212.	Viešųjų pirkimų tarnyba
213.	Lietuvos Respublikos vyriausioji rinkimų komisija
214.	Lietuvos Respublikos ryšių reguliavimo tarnyba
215.	Lietuvos Respublikos specialiųjų tyrimų tarnyba
216.	Lietuvos Respublikos vadovybės apsaugos tarnyba
217.	Lietuvos radijo ir televizijos komisija

Eil. Nr.	Juridinio asmens pavadinimas
218.	Valstybinė atominės energetikos saugos inspekcija
219.	Vyriausioji tarnybinės etikos komisija
220.	Lietuvos Respublikos žvalgybos kontrolierių įstaiga
221.	Alytaus apylinkės teismas
222.	Kauno apygardos teismas
223.	Kauno apylinkės teismas
224.	Klaipėdos apygardos teismas
225.	Klaipėdos apylinkės teismas
226.	Marijampolės apylinkės teismas
227.	Panevėžio apygardos teismas
228.	Panevėžio apylinkės teismas
229.	Plungės apylinkės teismas
230.	Šiaulių apygardos teismas
231.	Šiaulių apylinkės teismas
232.	Tauragės apylinkės teismas
233.	Telšių apylinkės teismas

Eil. Nr.	Juridinio asmens pavadinimas
234.	Utenos apylinkės teismas
235.	Regionų administracinis teismas
236.	Vilniaus apygardos teismas
237.	Vilniaus miesto apylinkės teismas
238.	Vilniaus regiono apylinkės teismas
239.	Lietuvos apeliacinis teismas
240.	Lietuvos vyriausiasis administracinis teismas
241.	Lietuvos Aukščiausiasis Teismas
242.	Lietuvos Respublikos Konstitucinis Teismas
Akmenės rajono savivaldybė	
243.	Akmenės rajono savivaldybės administracija
244.	Viešoji įstaiga Naujosios Akmenės ligoninė-sveikatos centras
Alytaus miesto savivaldybė	
245.	Alytaus miesto savivaldybės administracija
246.	Viešoji įstaiga Alytaus apskrities S. Kudirkos ligoninė
247.	Viešoji įstaiga Alytaus miesto savivaldybės pirminės sveikatos priežiūros centras
248.	Viešoji įstaiga Alytaus poliklinika

Eil. Nr.	Juridinio asmens pavadinimas
Alytaus rajono savivaldybė	
249.	Alytaus rajono savivaldybės administracija
250.	Alytaus rajono savivaldybės biudžetinė įstaiga Priešgaisrinės apsaugos tarnyba
251.	Viešoji įstaiga Alytaus rajono savivaldybės pirminės sveikatos priežiūros centras
Anykščių rajono savivaldybė	
252.	Anykščių rajono savivaldybės administracija
253.	Viešoji įstaiga Anykščių rajono savivaldybės ligoninė
254.	Viešoji įstaiga Anykščių rajono savivaldybės pirminės sveikatos priežiūros centras
Birštono savivaldybė	
255.	Birštono savivaldybės administracija
256.	Viešoji įstaiga Birštono pirminės sveikatos priežiūros centras
Biržų rajono savivaldybė	
257.	Biržų rajono savivaldybės administracija
258.	Biržų rajono savivaldybės priešgaisrinės apsaugos tarnyba
259.	Viešoji įstaiga Biržų ligoninė
260.	Viešoji įstaiga Biržų rajono savivaldybės poliklinika
Druskininkų savivaldybė	
261.	Druskininkų savivaldybės administracija

Eil. Nr.	Juridinio asmens pavadinimas
262.	Viešoji įstaiga Druskininkų ligoninė
Elektrėnų savivaldybė	
263.	Elektrėnų savivaldybės administracija
264.	Elektrėnų savivaldybės priešgaisrinė ir gelbėjimo tarnyba
265.	Elektrėnų savivaldybės visuomenės sveikatos biuras
266.	Viešoji įstaiga Abromiškių reabilitacijos ligoninė
267.	Viešoji įstaiga Elektrėnų ligoninė
268.	Viešoji įstaiga Elektrėnų savivaldybės sveikatos centras
Ignalinos rajono savivaldybė	
269.	Ignalinos rajono priešgaisrinė tarnyba
270.	Ignalinos rajono savivaldybės administracija
271.	Viešoji įstaiga Ignalinos rajono savivaldybės sveikatos centras
Jonavos rajono savivaldybė	
272.	Jonavos rajono savivaldybės administracija
273.	Viešoji įstaiga Jonavos ligoninė
274.	Viešoji įstaiga Jonavos pirminės sveikatos priežiūros centras
Joniškio rajono savivaldybė	

Eil. Nr.	Juridinio asmens pavadinimas
275.	Joniškio rajono savivaldybės administracija
276.	Joniškio rajono savivaldybės priešgaisrinė tarnyba
277.	Viešoji įstaiga Joniškio ligoninė
Jurbarko rajono savivaldybė	
278.	Jurbarko rajono priešgaisrinė tarnyba
279.	Jurbarko rajono savivaldybės administracija
280.	Jurbarko rajono savivaldybės visuomenės sveikatos biuras
281.	Viešoji įstaiga Eržvilko pirminės sveikatos priežiūros centras
282.	Viešoji įstaiga Jurbarko ligoninė
283.	Viešoji įstaiga Jurbarko rajono pirminės sveikatos priežiūros centras
284.	Viešoji įstaiga Seredžiaus ambulatorija
285.	Viešoji įstaiga Šimkaičių ambulatorija
286.	Viešoji įstaiga Viešvilės ambulatorija
Kaišiadorių rajono savivaldybė	
287.	Kaišiadorių rajono priešgaisrinė tarnyba
288.	Kaišiadorių rajono savivaldybės administracija
289.	Kaišiadorių pirminės sveikatos priežiūros centras

Eil. Nr.	Juridinio asmens pavadinimas
Kalvarijos savivaldybė	
290.	Kalvarijos priešgaisrinės apsaugos ir gelbėjimo tarnyba
291.	Kalvarijos savivaldybės administracija
292.	Viešojo įstaiga Kalvarijos savivaldybės sveikatos centras
Kauno miesto savivaldybė	
293.	Kauno miesto savivaldybės administracija
294.	Viešojo įstaiga K. Griniaus slaugos ir palaikomojo gydymo ligoninė
295.	VšĮ Kauno miesto poliklinika
Kauno rajono savivaldybė	
296.	Kauno rajono savivaldybės administracija
297.	Viešojo įstaiga Garliavos pirminės sveikatos priežiūros centras
298.	Viešojo įstaiga Pakaunės pirminės sveikatos priežiūros centras
299.	Viešojo įstaiga Vilkijos pirminės sveikatos priežiūros centras
Kazlų Rūdos savivaldybė	
300.	Kazlų Rūdos savivaldybės administracija
301.	Kazlų Rūdos savivaldybės Priešgaisrinė tarnyba
302.	Viešojo įstaiga Kazlų Rūdos pirminės sveikatos priežiūros centras

Eil. Nr.	Juridinio asmens pavadinimas
Kėdainių rajono savivaldybė	
303.	Kėdainių rajono savivaldybės administracija
304.	Kėdainių rajono savivaldybės priešgaisrinė tarnyba
305.	Viešoji įstaiga Kėdainių ligoninė
306.	Viešoji įstaiga Kėdainių pirminės sveikatos priežiūros centras
Kelmės rajono savivaldybė	
307.	Biudžetinė įstaiga Kelmės rajono priešgaisrinės saugos tarnyba
308.	Kelmės rajono savivaldybės administracija
309.	Viešoji įstaiga Kelmės ligoninė
310.	Viešoji įstaiga Tytuvėnų pirminės sveikatos priežiūros centras
311.	Viešoji įstaiga Kelmės rajono bendrosios praktikos gydytojų centras
312.	Viešoji įstaiga Šaukėnų ambulatorija
313.	Viešoji įstaiga Kelmės rajono pirminės sveikatos priežiūros centras
Klaipėdos miesto savivaldybė	
314.	Klaipėdos miesto savivaldybės administracija
315.	Viešoji įstaiga Klaipėdos medicininės slaugos ligoninė
316.	Viešoji įstaiga Klaipėdos vaikų ligoninė

Eil. Nr.	Juridinio asmens pavadinimas
317.	Viešoji įstaiga Klaipėdos miesto poliklinika
Klaipėdos rajono savivaldybė	
318.	Klaipėdos rajono savivaldybės administracija
319.	Klaipėdos rajono savivaldybės Gargždų ligoninė
320.	Klaipėdos rajono savivaldybės priešgaisrinė tarnyba
Kretingos rajono savivaldybė	
321.	Kretingos rajono savivaldybės administracija
322.	Kretingos rajono savivaldybės priešgaisrinė tarnyba
323.	Kretingos rajono savivaldybės viešoji įstaiga Kartenos pirminės sveikatos priežiūros centras
324.	Kretingos rajono savivaldybės viešoji įstaiga Kretingos ligoninė
325.	Kretingos rajono savivaldybės viešoji įstaiga Kretingos pirminės sveikatos priežiūros centras
326.	Kretingos rajono savivaldybės viešoji įstaiga Salantų pirminės sveikatos priežiūros centras
Kupiškio rajono savivaldybė	
327.	Kupiškio rajono savivaldybės administracija
328.	Kupiškio rajono savivaldybės priešgaisrinė tarnyba
329.	Viešoji įstaiga Kupiškio ligoninė
330.	Viešoji įstaiga Kupiškio rajono savivaldybės pirminės asmens sveikatos priežiūros centras

Eil. Nr.	Juridinio asmens pavadinimas
Lazdijų rajono savivaldybė	
331.	Lazdijų rajono savivaldybės administracija
332.	Lazdijų rajono savivaldybės priešgaisrinė tarnyba
333.	Viešoji įstaiga Lazdijų ligoninė
Marijampolės savivaldybė	
334.	Marijampolės savivaldybės administracija
335.	Viešoji įstaiga Marijampolės ligoninė
336.	Viešoji įstaiga Marijampolės pirminės sveikatos priežiūros centras
Mažeikių rajono savivaldybė	
337.	Mažeikių rajono savivaldybės administracija
338.	Viešoji įstaiga Mažeikių ligoninė
339.	Viešoji įstaiga Mažeikių pirminės sveikatos priežiūros centras
340.	Viešoji įstaiga Sedos pirminės sveikatos priežiūros centras
Molėtų rajono savivaldybė	
341.	Molėtų rajono savivaldybės administracija
342.	Viešoji įstaiga Molėtų rajono sveikatos centras
Neringos savivaldybė	
343.	Neringos savivaldybės administracija

Eil. Nr.	Juridinio asmens pavadinimas
344.	Viešoji įstaiga Neringos pirminės sveikatos priežiūros centras
Pagėgių savivaldybė	
345.	Pagėgių savivaldybės administracija
346.	Pagėgių savivaldybės priešgaisrinė tarnyba
347.	Viešoji įstaiga Pagėgių pirminės sveikatos priežiūros centras
Pakruojo rajono savivaldybė	
348.	Pakruojo rajono savivaldybės administracija
349.	Viešoji įstaiga Pakruojo ligoninė
Palangos miesto savivaldybė	
350.	Palangos miesto savivaldybės administracija
351.	Viešoji įstaiga Palangos asmens sveikatos priežiūros centras
Panevėžio miesto savivaldybė	
352.	Panevėžio miesto savivaldybės administracija
353.	Viešoji įstaiga Panevėžio palaikomojo gydymo ir slaugos ligoninė
354.	Viešoji įstaiga Panevėžio miesto poliklinika
355.	Viešoji įstaiga Panevėžio miesto odontologijos poliklinika
356.	Viešoji įstaiga Panevėžio fizinės medicinos ir reabilitacijos centras
Panevėžio rajono savivaldybė	

Eil. Nr.	Juridinio asmens pavadinimas
357.	Panevėžio rajono savivaldybės administracija
358.	Panevėžio rajono savivaldybės priešgaisrinė tarnyba
359.	Panevėžio rajono savivaldybės visuomenės sveikatos biuras
360.	Viešoji įstaiga Panevėžio rajono savivaldybės poliklinika
361.	Viešoji įstaiga Velžio komunalinis ūkis
Pasvalio rajono savivaldybė	
362.	Pasvalio rajono savivaldybės administracija
363.	Pasvalio rajono savivaldybės priešgaisrinė tarnyba
364.	Viešoji įstaiga Pasvalio ligoninė
365.	Viešoji įstaiga Pasvalio pirminės asmens sveikatos priežiūros centras
Plungės rajono savivaldybė	
366.	Plungės rajono savivaldybės administracija
367.	Plungės rajono savivaldybės priešgaisrinės apsaugos tarnyba
368.	Viešoji įstaiga Plungės rajono savivaldybės ligoninė
Prienų rajono savivaldybė	
369.	Prienų rajono savivaldybės administracija
370.	Prienų rajono savivaldybės priešgaisrinė tarnyba

Eil. Nr.	Juridinio asmens pavadinimas
371.	Viešoji įstaiga Prienų ligoninė
372.	Viešoji įstaiga Prienų rajono pirminės sveikatos priežiūros centras
Radviliškio rajono savivaldybė	
373.	Radviliškio rajono savivaldybės administracija
374.	Viešoji įstaiga Radviliškio ligoninė
375.	Viešoji įstaiga Radviliškio rajono pirminės sveikatos priežiūros centras
376.	Viešoji įstaiga Baisogalos pirminės sveikatos priežiūros centras
377.	Viešoji įstaiga Šeduvos pirminės sveikatos priežiūros centras
Raseinių rajono savivaldybė	
378.	Raseinių priešgaisrinės saugos tarnyba
379.	Raseinių rajono savivaldybės administracija
380.	Viešoji įstaiga Raseinių ligoninė
381.	Viešoji įstaiga Raseinių pirminės sveikatos priežiūros centras
382.	Viešoji įstaiga Ariogalos pirminės sveikatos priežiūros centras
Rietavo savivaldybė	
383.	Rietavo savivaldybės administracija
384.	Rietavo savivaldybės priešgaisrinė tarnyba

Eil. Nr.	Juridinio asmens pavadinimas
385.	Viešoji įstaiga Rietavo pirminės sveikatos priežiūros centras
Rokiškio rajono savivaldybė	
386.	Rokiškio rajono savivaldybės administracija
387.	Rokiškio rajono savivaldybės priešgaisrinė tarnyba
388.	Viešoji įstaiga Rokiškio rajono ligoninė
389.	Viešoji įstaiga Rokiškio pirminės asmens sveikatos priežiūros centras
Šakių rajono savivaldybė	
390.	Šakių rajono savivaldybės administracija
391.	Šakių rajono savivaldybės visuomenės sveikatos biuras
392.	Viešoji įstaiga Kidulių ambulatorija
393.	Viešoji įstaiga Kudirkos Naumiesčio pirminės sveikatos priežiūros centras
394.	Viešoji įstaiga Lekėčių ambulatorija
395.	Viešoji įstaiga Šakių ligoninė
396.	Viešoji įstaiga Šakių pirminės asmens sveikatos priežiūros centras
Šalčininkų rajono savivaldybė	
397.	Šalčininkų rajono savivaldybės administracija
398.	Šalčininkų rajono savivaldybės priešgaisrinė tarnyba

Eil. Nr.	Juridinio asmens pavadinimas
399.	Viešoji įstaiga Šalčininkų pirminės sveikatos priežiūros centras
400.	Viešoji įstaiga Šalčininkų rajono savivaldybės ligoninė
Šiaulių miesto savivaldybė	
401.	Šiaulių miesto savivaldybės administracija
402.	Viešoji įstaiga Šiaulių centro poliklinika
403.	Viešoji įstaiga Dainų pirminės sveikatos priežiūros centras
404.	Viešoji įstaiga Šiaulių ilgalaikio gydymo ir geriatrijos centras
405.	Viešoji įstaiga Šiaulių reabilitacijos centras
406.	Šiaulių miesto savivaldybės visuomenės sveikatos biuras
Šiaulių rajono savivaldybė	
407.	Šiaulių rajono savivaldybės administracija
408.	Šiaulių rajono savivaldybės priešgaisrinė tarnyba
409.	Viešoji įstaiga Šiaulių rajono savivaldybės sveikatos centras
Šilalės rajono savivaldybė	
410.	Šilalės rajono savivaldybės administracija
411.	Šilalės rajono savivaldybės priešgaisrinė tarnyba
412.	Viešoji įstaiga Šilalės rajono savivaldybės sveikatos centras

Eil. Nr.	Juridinio asmens pavadinimas
413.	Viešoji įstaiga Kaltinėnų pirminės sveikatos priežiūros centras
Šilutės rajono savivaldybė	
414.	Šilutės rajono savivaldybės administracija
415.	Šilutės rajono savivaldybės priešgaisrinė tarnyba
416.	Viešoji įstaiga Šilutės ligoninė
417.	Viešoji įstaiga Šilutės pirminės sveikatos priežiūros centras
Širvintų rajono savivaldybė	
418.	Širvintų rajono savivaldybės administracija
419.	Širvintų rajono savivaldybės priešgaisrinė tarnyba
420.	Viešoji įstaiga Širvintų rajono savivaldybės sveikatos centras
Skuodo rajono savivaldybė	
421.	Skuodo rajono savivaldybės administracija
422.	Skuodo rajono savivaldybės priešgaisrinė tarnyba
423.	Skuodo pirminės sveikatos priežiūros centras
424.	Viešoji įstaiga Mosėdžio pirminės sveikatos priežiūros centras
Švenčionių rajono savivaldybė	
425.	Priešgaisrinės apsaugos tarnyba prie Švenčionių rajono savivaldybės administracijos
426.	Švenčionių rajono savivaldybės administracija

Eil. Nr.	Juridinio asmens pavadinimas
427.	Viešoji įstaiga Švenčionių rajono sveikatos centras
Tauragės rajono savivaldybė	
428.	Tauragės rajono savivaldybės administracija
429.	Tauragės rajono savivaldybės priešgaisrinė tarnyba
430.	Viešoji įstaiga Tauragės ligoninė
431.	Viešoji įstaiga Tauragės rajono pirminės sveikatos priežiūros centras
Telšių rajono savivaldybė	
432.	Telšių rajono savivaldybės administracija
433.	Telšių rajono savivaldybės priešgaisrinė tarnyba
434.	Viešoji įstaiga Regioninė Telšių ligoninė
435.	Telšių rajono pirminės sveikatos priežiūros centras
Trakų rajono savivaldybė	
436.	Trakų rajono priešgaisrinė gelbėjimo įstaiga
437.	Trakų rajono savivaldybės administracija
438.	Viešoji įstaiga Onuškio palaikomojo gydymo ir slaugos ligoninė
439.	Viešoji įstaiga Trakų ligoninė
440.	Viešoji įstaiga Lentvario ambulatorija

Eil. Nr.	Juridinio asmens pavadinimas
441.	Viešoji įstaiga Trakų pirminės sveikatos priežiūros centras
Ukmergės rajono savivaldybė	
442.	Ukmergės rajono savivaldybės administracija
443.	Ukmergės rajono savivaldybės priešgaisrinė tarnyba
444.	Viešoji įstaiga Ukmergės ligoninė
445.	Viešoji įstaiga Ukmergės pirminės sveikatos priežiūros centras
Utenos rajono savivaldybė	
446.	Utenos rajono savivaldybės administracija
447.	Utenos rajono savivaldybės priešgaisrinė tarnyba
448.	Utenos rajono savivaldybės visuomenės sveikatos biuras
449.	Viešoji įstaiga Utenos ligoninė
450.	Viešoji įstaiga Utenos pirminės sveikatos priežiūros centras
451.	Viešoji įstaiga Šv. Klaros palaikomojo gydymo ir slaugos ligoninė
Varėnos rajono savivaldybė	
452.	Varėnos rajono savivaldybės administracija
453.	Varėnos rajono savivaldybės priešgaisrinės apsaugos tarnyba
454.	Viešoji įstaiga Varėnos sveikatos centras

Eil. Nr.	Juridinio asmens pavadinimas
Vilkaviškio rajono savivaldybė	
455.	Biudžetinė įstaiga Vilkaviškio rajono priešgaisrinė tarnyba
456.	Viešoji įstaiga Vilkaviškio ligoninė
457.	Viešoji įstaiga Vilkaviškio pirminės sveikatos priežiūros centras
458.	Vilkaviškio rajono savivaldybės administracija
Vilniaus miesto savivaldybė	
459.	Viešoji įstaiga Antakalnio poliklinika
460.	Viešoji įstaiga Centro poliklinika
461.	Viešoji įstaiga Grigiškių sveikatos priežiūros centras
462.	Viešoji įstaiga Naujosios Vilnios poliklinika
463.	Viešoji įstaiga Karoliniškių poliklinika
464.	Viešoji įstaiga Šeškinės poliklinika
465.	Viešoji įstaiga Vilniaus miesto psichikos sveikatos centras
466.	Viešoji įstaiga Mykolo Marcinkevičiaus ligoninė
467.	Viešoji įstaiga Šv. Roko ligoninė
468.	Viešoji įstaiga Vilkpėdės ligoninė

Eil. Nr.	Juridinio asmens pavadinimas
469.	Viešoji įstaiga Vilniaus miesto klinikinė ligoninė
470.	Vilniaus miesto savivaldybės administracija
471.	Vilniaus miesto savivaldybės visuomenės sveikatos biuras
472.	Viešoji įstaiga Vilniaus rajono Nemenčinės poliklinika
Vilniaus rajono savivaldybė	
473.	Vilniaus rajono savivaldybės administracija
474.	Vilniaus rajono savivaldybės priešgaisrinė tarnyba
475.	Viešoji įstaiga Vilniaus rajono centrinė poliklinika
Visagino savivaldybė	
476.	Viešoji įstaiga Visagino ligoninė
477.	Visagino savivaldybės administracija
Zarasų rajono savivaldybė	
478.	Zarasų priešgaisrinės apsaugos tarnyba
479.	Zarasų rajono savivaldybės administracija
480.	Zarasų rajono savivaldybės viešoji įstaiga Sveikatos centras

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2018 m. rugpjūčio 13 d. nutarimu Nr. 818
(Lietuvos Respublikos Vyriausybės
2024 m. lapkričio 6 d. nutarimo Nr. 945
redakcija)

**ATLYGINIMO UŽ NAUDOJIMĄSI SAUGIUOJU VALSTYBINIU DUOMENŲ
PERDAVIMO TINKLU TEIKIAMOMIS PAPILDOMOMIS ELEKTRONINIŲ
RYŠIŲ IR KIBERNETINIO SAUGUMO PASLAUGOMIS DYDŽIŲ NUSTATYMO
KRITERIJŲ IR ATLYGINIMO APSKAIČIAVIMO TVARKOS APRAŠAS**

**I SKYRIUS
BENDROSIOS NUOSTATOS**

1. Atlyginimo už naudojimąsi Saugiuoju valstybiniu duomenų perdavimo tinklu teikiamomis papildomomis elektroninių ryšių ir kibernetinio saugumo paslaugomis dydžių nustatymo kriterijų ir atlyginimo apskaičiavimo tvarkos aprašas (toliau – Aprašas) nustato atlyginimo už naudojimąsi Saugiuoju valstybiniu duomenų perdavimo tinklu (toliau – Saugusis tinklas) teikiamomis papildomomis elektroninių ryšių ir kibernetinio saugumo paslaugomis (toliau – papildomos paslaugos) dydžių (toliau – atlyginimo dydžiai) nustatymo kriterijus bei atlyginimo dydžių apskaičiavimo, derinimo ir tvirtinimo tvarką.

2. Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos elektroninių ryšių įstatyme.

**II SKYRIUS
ATLYGINIMO DYDŽIŲ NUSTATYMO KRITERIJAI IR ATLYGINIMO DYDŽIŲ
APSKAIČIAVIMAS**

3. Saugiojo tinklo tvarkytojas iki kalendorinių metų pabaigos apskaičiuoja atlyginimo dydžius pagal Aprašo 4 punkte nurodytus atlyginimo dydžių nustatymo kriterijus.

4. Atlyginimo dydžių nustatymo kriterijai:

4.1. ekonomiškai pagrįsta papildomos paslaugos savikaina (išlaidos), pagrindžiama papildomą paslaugą teikiančio Saugiojo tinklo tvarkytojo praėjusių kalendorinių metų materialinėmis ir joms prilygintomis sąnaudomis (ilgalaikio materialiojo turto nusidėvėjimo ir nematerialiojo turto amortizacijos, komunalinių paslaugų, elektroninių ryšių paslaugų, remonto, elektroninių ryšių tinklo išlaikymo sąnaudos) ir darbo sąnaudomis (darbo užmokesčio, socialinio draudimo įmokų sąnaudos), patiriamomis teikiant konkrečią papildomą paslaugą;

4.2. numatomos teikti papildomos paslaugos savikaina (išlaidos), pagrindžiama prognozuojamomis sąnaudomis, nurodytomis Aprašo 4.1 papunktyje.

5. Apskaičiuojant atlyginimo dydžius, leidžiama įtraukti tik būtinas ir pagrįstas sąnaudas, tiesiogiai susijusias su teikiamomis papildomomis paslaugomis.

6. Saugiojo tinklo tvarkytojas su auditoriumi ar audito įmone, kaip jie apibrėžti Lietuvos Respublikos finansinių ataskaitų audito ir kitų užtikrinimo paslaugų įstatyme (toliau – audito įmonė), sudaro papildomų paslaugų teikimo sąnaudų patikrinimo (toliau – patikrinimas) sutartį.

7. Saugiojo tinklo tvarkytojas, apskaičiavęs atlyginimo dydžius, ne vėliau kaip per 1 mėnesį nuo kalendorinių metų pabaigos audito įmonei pateikia visą detalią informaciją, kuria pagrindžiamos papildomų paslaugų teikimo sąnaudos, ir kitą informaciją, reikalingą papildomų paslaugų teikimo sąnaudoms patikrinti.

8. Audito įmonė iš Saugiojo tinklo tvarkytojo turi teisę gauti papildomų duomenų ir paaiškinimų, kurių reikia papildomų paslaugų teikimo sąnaudoms patikrinti.

9. Audito įmonei atlikus patikrinimą ir pateikus patikrinimo ataskaitą, kurioje nurodyta papildomų paslaugų teikimo sąnaudų apskaičiavimo trūkumų, Saugiojo tinklo tvarkytojas privalo pašalinti audito įmonės nurodytus trūkumus. Šiame punkte nurodytu atveju turi būti gauta papildoma audito įmonės patikrinimo ataskaita.

10. Audito įmonei atlikus patikrinimą ir nenustačius papildomų paslaugų teikimo sąnaudų apskaičiavimo trūkumų, Saugiojo tinklo tvarkytojas per Kibernetinio saugumo įstatymo 37 straipsnio 8 dalyje nurodytą terminą pateikia informaciją apie apskaičiuotus atlyginimo dydžius ir patikrintus duomenis apie patirtas sąnaudas Lietuvos Respublikos Vyriausybės įgaliotai institucijai.

11. Vyriausybės įgaliota institucija nepradedą rengti išvados, kol nėra gauta visa išvada pateikti reikalinga informacija. Vyriausybės įgaliota institucija per 15 darbo dienų nuo visos išvados pateikti reikalingos informacijos gavimo dienos pateikia išvadą, ar atlyginimo dydžiai apskaičiuoti atsižvelgiant į Aprašo 4 punkte nurodytus atlyginimo dydžių nustatymo kriterijus. Jei Vyriausybės įgaliota institucija nustato, kad atlyginimo dydžiai apskaičiuoti neatsižvelgiant į Aprašo 4 punkte nurodytus kriterijus, informuoja Saugiojo tinklo tvarkytoją, kuris per ne ilgesnį nei 10 darbo dienų terminą nuo tokios informacijos gavimo dienos turi ištaisyti nustatytus trūkumus ir pakartotinai pateikti patikrintus duomenis apie patirtas sąnaudas ir atlyginimo dydžius.

12. Saugiojo tinklo tvarkytojas, gavęs Vyriausybės įgaliotos institucijos išvadą, kad atlyginimo dydžiai apskaičiuoti atsižvelgiant į Aprašo 4 punkte nurodytus atlyginimo dydžių nustatymo kriterijus, per 10 darbo dienų nuo išvados gavimo dienos teikia apskaičiuotus atlyginimo dydžius ir visą susijusią informaciją krašto apsaugos ministrui.

13. Atlyginimo dydžiai perskaičiuojami kasmet. Patvirtinti atlyginimo dydžiai keičiami tik tais atvejais, kai jie skiriasi nuo naujai apskaičiuotų atlyginimo dydžių. Naujai apskaičiuoti dydžiai turi būti patvirtinti ne vėliau kaip per 3 mėnesius nuo kalendorinių metų pabaigos.

III SKYRIUS BAIGIAMOSIOS NUOSTATOS

14. Atlyginimo dydžiai, patikrinimo ataskaitos ir Vyriausybės įgaliotos institucijos išvados viešai skelbiami Saugiojo tinklo tvarkytojo interneto svetainėje.

Priedų pakeitimai:

Nacionalinio kibernetinių incidentų valdymo plano 1 priedas

Nacionalinio kibernetinių incidentų valdymo plano 2 priedas

Nacionalinio kibernetinių incidentų valdymo plano 3 priedas

Nacionalinio kibernetinių incidentų valdymo plano 4 priedas

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

3.

Lietuvos Respublikos Vyriausybė, Nutarimas

Nr. [1298](#), 2020-11-18, paskelbta TAR 2020-11-23, i. k. 2020-24708

Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo

4.

Lietuvos Respublikos Vyriausybė, Nutarimas

Nr. [574](#), 2023-07-19, paskelbta TAR 2023-07-19, i. k. 2023-14859

Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo

5.

Lietuvos Respublikos Vyriausybė, Nutarimas

Nr. [945](#), 2024-11-06, paskelbta TAR 2024-11-11, i. k. 2024-19589

Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo