LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

N U T A R I M A S

DĖL ELEKTRONINĖS INFORMACIJOS SAUGOS (KIBERNETINIO SAUGUMO) PLĖTROS 2011–2019 METAIS PROGRAMOS PATVIRTINIMO

2011 m. birželio 29 d. Nr. 796
Vilnius

Įgyvendindama Lietuvos Respublikos Vyriausybės 2008–2012 metų programos įgyvendinimo priemonių, patvirtintų Lietuvos Respublikos Vyriausybės 2009 m. vasario 25 d. nutarimu Nr. 189 (Žin., 2009, Nr. 33-1268), 3 lentelės 65 punktą, Lietuvos Respublikos Vyriausybė n u t a r i a:

1. Patvirtinti Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą (pridedama).

2. Pasiūlyti Lietuvos Respublikos valstybės saugumo departamentui ir Lietuvos Respublikos ryšių reguliavimo tarnybai dalyvauti įgyvendinant Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą.

MINISTRAS PIRMININKAS ANDRIUS KUBILIUS

TEISINGUMO MINISTRAS,
PAVADUOJANTIS VIDAUS REIKALŲ MINISTRĄ REMIGIJUS ŠIMAŠIUS

_____

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2011 m. birželio 29 d. nutarimu Nr. 796

ELEKTRONINĖS INFORMACIJOS SAUGOS (KIBERNETINIO SAUGUMO) PLĖTROS 2011–2019 METAIS PROGRAMA

I. BENDROSIOS NUOSTATOS

1. Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa (toliau – Programa) parengta atsižvelgiant į tai, kad valstybės ir visuomenės gyvenime vis didesnę reikšmę įgyja informacinėmis ir ryšių technologijomis tvarkoma ir perduodama elektroninė informacija, atsiradusios elektroninės informacijos tvarkymo galimybės paskatino nacionalinių ir globalių informacinių visuomenių atsiradimą ir sudarė sąlygas toliau modernizuoti šalių ūkius ir efektyviau valdyti valstybę, tačiau tuo pačiu metu į elektroninę formą perkeliama vis daugiau informacijos, sparčiai automatizuojami įvairūs šalies valdymo ir ūkio veiklos procesai, globali kibernetinė erdvė ir joje teikiamos viešosios paslaugos tapo patraukliu atskirų asmenų, nusikalstamų grupuočių, politinių jėgų ir kitų subjektų taikiniu.

2. Programos paskirtis – nustatyti elektroninės informacijos saugos (kibernetinio saugumo) plėtros tikslus ir uždavinius, kad būtų užtikrintas elektroninės informacijos ir kibernetinėje erdvėje teikiamų paslaugų konfidencialumas, vientisumas ir prieinamumas, elektroninių ryšių tinklų, informacinių sistemų ir ypatingos svarbos informacinės infrastruktūros apsauga nuo incidentų ir kibernetinių atakų, asmens duomenų ir privatumo apsauga, taip pat nustatyti uždavinius, kurių įgyvendinimas leistų užtikrinti bendrą kibernetinės erdvės ir joje veiklą vykdančių subjektų saugumą.

3. Programos strateginis tikslas – plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 procentus visų valstybės informacinių išteklių, vidutinis ypatingos svarbos informacinės infrastruktūros incidentų likvidavimo laikas sumažėtų iki 0,5 valandos, o Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis pasiektų 60 procentų.

4. Programoje vartojamos sąvokos:

Informaciniai ištekliai – informacijos, kurią valdo informacinės visuomenės nariai ir kuri apdorojama informacinių technologijų priemonėmis, ir šią informaciją apdorojančių informacinių technologijų priemonių visuma.

Incidentas – įvykis, veiksmas ar neveikimas, kuris sudaro ar gali sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos ar elektroninių ryšių tinklo, sutrikdyti ar pakeisti (įskaitant valdymo perėmimą) informacinės sistemos ar elektroninių ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, taip pat sudaro ar gali sudaryti sąlygas pasisavinti, paskelbti, platinti ar kitaip naudoti neviešąją elektroninę informaciją tokios teisės neturintiems asmenims.

Ypatingos svarbos informacinė infrastruktūra – elektroninių ryšių tinklas, informacinė sistema ar informacinių sistemų grupė, kurioje įvykęs incidentas padaro ar gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui ar visuomenės gerovei.

5. Programa atitinka Europos Komisijos 2009 m. kovo 30 d. komunikate KOM (2009) 149 „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“ išdėstytas veiklos kryptis.

II. TIKSLAI, UŽDAVINIAI, VERTINIMO KRITERIJAI IR JŲ REIKŠMĖS

6. Nustatomi šie Programos įgyvendinimo tikslai:

6.1. Pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas.

Šio tikslo siekiama, nes, išskyrus valstybinį sektorių (Lietuvos Respublikos Vyriausybei atskaitingose įstaigose ir institucijose), nėra sukurta elektroninės informacijos saugos valdymo koordinavimo sistema. Vidaus reikalų ministerijai trūksta įgaliojimų tinkamai vykdyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo kontrolę ir koordinavimą, valdymo ir priežiūros struktūra valstybės ir valstybės institucijų mastu nėra hierarchinė, trūksta Lietuvos viešojo ir privataus sektoriaus subjektų bendradarbiavimo, tai neleidžia veiksmingai planuoti elektroninės informacijos saugos (kibernetinio saugumo) srities plėtrą; informacinių technologijų esami ir nuolat aptinkami nauji pažeidžiamumai, jų laiku nepašalinus, sudaro sąlygas sutrikdyti informacinių išteklių, taip pat ypatingos svarbos informacinės infrastruktūros objektų funkcionavimą, o šių pažeidžiamumų aptikimo ir šalinimo veiksmingumas didėja centralizuojant šią veiklą. Atitiktis keliamiems elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams užtikrina informacinių išteklių saugos valdymą pagal tarptautinių standartų reikalavimus ir gerosios praktikos pavyzdžius, tačiau Lietuvoje nesuformuota veiksminga atitikties valdymo struktūra; organizacijos informacinės brandos modelis leidžia informacinių išteklių valdytojams geriau suvokti informacinių išteklių saugos poreikį ir veiksmingiau valdyti informacinių išteklių saugą. Įvairios valstybės ir visuomenės veiklos sritys nevienodai priklausomos nuo informacinių išteklių ir paslaugų naudojimo, todėl, siekiant veiksmingai naudoti lėšas, būtina telkti pastangas ir informacinius išteklius tose srityse, kuriose ši priklausomybė didesnė; nusikalstamų veikų kibernetinėje erdvėje sparčiai daugėja, o didelio masto incidentai kibernetinėje erdvėje gali sukelti nacionalinio masto krizę.

Nėra įstatymo, kuriuo reglamentuojama elektroninės informacijos sauga (kibernetinis saugumas), reglamentavimas žemesnės teisinės galios teisės aktais yra fragmentiškas ir neapima visų informacinės visuomenės narių, kartu nesukurta teisinė bazė, sudaranti prielaidas veiksmingai kovoti su incidentais viešuosiuose elektroninių ryšių tinkluose, elektroninių ryšių ir interneto prieigos paslaugų teikėjams nėra privaloma pranešti apie incidentus nacionaliniam elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padaliniui CERT-LT (toliau – nacionalinis CERT-LT). Atitinkamai nacionalinio CERT-LT nurodymai paslaugų teikėjams dėl incidentų šalinimo taip pat nėra privalomi, nesukurta teisinė bazė, kuri reglamentuotų tapatybės nustatymo priemonių naudojimą, siekiant mažinti tapatybės klastojimo ir pasisavinimo kibernetinėje erdvėje pavojų.

Interneto ir kitų informacinės infrastruktūros paslaugų teikėjų teikiamos paslaugos dažnai neužtikrina paslaugų naudotojų saugos. Ekonominiu sunkmečiu elektroninės informacijos saugai (kibernetiniam saugumui) skiriama nepakankamai dėmesio ir informacinių išteklių, o taikant kolektyvinės saugos principą būtų veiksmingiau naudojami informaciniai ištekliai; nėra sukurtas informacinių išteklių ir infrastruktūros rezervas, skirtas ypatingos svarbos infrastruktūros ir informacinių išteklių veikimo palaikymui kritiniais atvejais. Patikimas tapatybės nustatymas sumažina didelės dalies grėsmių, susijusių su kibernetine erdve, keliamą riziką, skatina naudotojų pasitikėjimą kibernetine erdve.

Saugia kibernetine erdve (t. y. elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimu) yra suinteresuoti visi subjektai, kurių veikla susijusi su kibernetinėje erdvėje teikiamomis paslaugomis (valstybės institucijos, privatūs ūkio subjektai, akademinė bendruomenė ir kiti). Bendradarbiaujant vykdomi elektroninės informacijos saugos (kibernetinio saugumo) projektai leidžia užtikrinti visų dalyvaujančių šalių interesų apsaugą.

Kibernetinė erdvė yra globali, neturinti nacionalinių ribų, taigi grėsmių plitimas joje didelis. Europos Sąjunga ir NATO skiria daug dėmesio elektroninės informacijos ir ypatingos svarbos informacinės infrastruktūros saugai. Kolektyvinės apsaugos principu tikslinga vadovautis ne tik nacionaliniu, bet ir tarptautiniu lygiu. Aukštos kompetencijos specialistų

bendradarbiavimas, keitimasis turima informacija ir patirtimi yra būtina veiksmingos išankstinio perspėjimo ir prevencinės veiklos sąlyga.

6.2. Užtikrinti veiksmingą ypatingos svarbos informacinės infrastruktūros funkcionavimą.

Šio tikslo siekiama, nes ypatingos svarbos informacinės infrastruktūros saugumas užtikrinamas tik žinybiniu lygmeniu, nesuformuota koordinavimo struktūra, neišanalizuoti šios infrastruktūros objektų tarpusavio ryšiai ir sutrikdymo poveikis nacionaliniu mastu, nevykdomas veiklos tęstinumo planavimas. Bandymų įsilaužti būdas (angl. – *penetration test*) yra objektyviausias būdas įsitikinti, ar tinkamai veikia saugos sistema, tačiau jo taikymas nėra reglamentuotas, nėra tokių bandymų praktikos. Veiksminga stebėsenos sistema sudaro sąlygas vykdyti incidentų prevenciją.

6.3. Siekti užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje.

Šio tikslo siekiama, nes ne visi elektroninės informacijos naudotojai rūpinasi elektroninės informacijos sauga (kibernetiniu saugumu), stinga ir tikėtina, kad ateityje vis labiau stigs kvalifikuotų elektroninės informacijos saugos specialistų. Bazinės elektroninės informacijos saugos (kibernetinio saugumo) žinios ir įrankiai leidžia naudotojams išvengti daugelio grėsmių kibernetinėje erdvėje.

Kibernetinės erdvės saugumui užtikrinti būtina nenutrūkstamai veikianti ir tinkamai valdoma sistema, apimanti visą incidentų gyvavimo ciklą: išankstinio perspėjimo, prevencijos, aptikimo, likvidavimo ir tyrimo fazes. Siekiant kovoti su kenksminga programine įranga nuotoliniu būdu valdomų kompiuterių tinklais ar kitais kenkėjiškos veiklos kibernetinėje erdvėje būdais, veiksminga blokuoti interneto prieigą kenkėjišką veiklą vykdantiems asmenims ir (ar) įrenginiams. Šiuo metu visuomenėje yra susiformavęs stereotipas dėl nebaudžiamumo už neteisėtus veiksmus kibernetinėje erdvėje, todėl svarbu šį stereotipą panaikinti.

Kibernetinės atakos, kurių šaltinis yra užsienyje, gali ir turi būti stabdomos ties virtualiu Lietuvos kibernetinės erdvės perimetru, siekiant išvengti jų poveikio šalies vidaus elektroninių ryšių tinkluose. Lietuvos interneto srauto mainų (ISM) mazgas yra natūraliai susiformavęs subjektas, kuriame patogu ir veiksminga telkti Lietuvos kibernetinės erdvės (taip pat virtualaus perimetro) apsaugos pajėgumus.

Kibernetinėje erdvėje teikiamų paslaugų srityje vyrauja jų unifikavimo ir centralizavimo tendencija, siekiant įgyvendinti vieno langelio principą; tikslinga šia tendencija pasinaudoti ir užtikrinant šių paslaugų saugą. Naudotojų pasitikėjimas kibernetinėje erdvėje teikiamomis paslaugomis yra vienas svarbiausių veiksnių šių paslaugų populiarumui ir tolesnei plėtrai.

7. Programos 6.1 punkte nurodytam tikslui pasiekti reikia įgyvendinti šiuos uždavinius:

7.1. tobulinti elektroninės informacijos saugos (kibernetinio saugumo) koordinavimą ir priežiūrą;

7.2. tobulinti elektroninės informacijos saugos (kibernetinio saugumo) teisinį reglamentavimą;

7.3. plėsti ir tobulinti saugią valstybės informacinę infrastruktūrą;

7.4. skatinti elektroninės informacijos saugos (kibernetinio saugumo) projektų įgyvendinimą;

7.5. plėtoti tarptautinį bendradarbiavimą elektroninės informacijos saugos (kibernetinio saugumo) srityje.

8. Programos 6.2 punkte nurodytam tikslui pasiekti reikia įgyvendinti šį uždavinį – užtikrinti ypatingos svarbos informacinės infrastruktūros saugumą.

9. Programos 6.3 punkte nurodytam tikslui pasiekti reikia įgyvendinti šiuos uždavinius:

9.1. kelti elektroninės informacijos saugos (kibernetinio saugumo) kultūrą;

9.2. stiprinti Lietuvos kibernetinės erdvės saugumą;

9.3. užtikrinti virtualaus Lietuvos kibernetinės erdvės perimetro apsaugą nuo išorinių kibernetinių atakų;

9.4. stiprinti kibernetinėje erdvėje teikiamų paslaugų saugumą.

10. Programos įgyvendinimo vertinimo kriterijai ir siekiamos jų reikšmės 2011, 2015 ir 2019 metais pateikiami Programos priede.

11. Atsižvelgiant į tai, kad Programa apima vieną vidaus reikalų ministrui pavestą valdymo sritį, Programos finansavimo Europos Sąjungos lėšomis skirstyti tarp Programą įgyvendinančių institucijų nenumatoma.

III. PROGRAMOS ĮGYVENDINIMAS

12. Programos įgyvendinimą koordinuoja Vidaus reikalų ministerija (toliau – Programos koordinatorius).

13. Už Programos tikslų ir uždavinių įgyvendinimą atsako institucijos ir įstaigos, nurodytos Programos priede.

14. Programos įgyvendinime dalyvaujančios institucijos:

14.1. atsižvelgdamos į Programoje numatytus uždavinius ir siekiamus rezultatus, numato rezultato pasiekimo reikšmę planuojamu laikotarpiu, pasirenka priemones ir suplanuoja lėšas, įtraukia jas į strateginius veiklos planus ir (arba) metinius veiklos planus ir kasmet iki rugpjūčio 1 d. šią informaciją pateikia Programos koordinatoriui;

14.2. kasmet iki vasario 1 d. pateikia Programos koordinatoriui informaciją apie vykdytas priemones ir pasiektus rezultatus.

15. Programos koordinatorius:

15.1. prižiūri, kaip įgyvendinami Programos strateginis tikslas, tikslai, uždaviniai, atlieka tarpinę Programoje numatytų uždavinių ir jų vertinimo kriterijų reikšmių pokyčių peržiūrą ir prireikus inicijuoja Programos atnaujinimą;

15.2. teikia informaciją apie Programos įgyvendinimą ir rezultatus Programos koordinatoriaus metinėje veiklos ataskaitoje.

16. Programai įgyvendinti papildomų teisės aktų, išskyrus nurodytus Programos 14.1 punkte, parengti nereikės.

_____

Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos priedas

ELEKTRONINĖS INFORMACIJOS SAUGOS (KIBERNETINIO SAUGUMO) PLĖTROS 2011–2019 METAIS PROGRAMOS ĮGYVENDINIMO VERTINIMO KRITERIJAI IR SIEKIAMOS JŲ REIKŠMĖS

Eil. Nr.	Tikslas	Uždavinys	Vertinimo kriterijus	Rodiklis 2011 metais	Rodiklis 2015 metais	Rodiklis 2019 metais	Už kriterijaus įgyvendinimą atsakinga institucija
1.	1. Pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas		Saugos reikalavimus atitinkančių valstybės informacinių išteklių dalis, procentais	–	95	98	pagal kompetenciją visos šio priedo 3–29 punktuose nurodytos institucijos
2.		1.1. tobulinti elektroninės informacijos saugos (kibernetinio saugumo) koordinavimą ir priežiūrą	Išteklių, kurių saugumas yra prižiūrimas institucijos, paskirtos esminius su elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimu susijusius reikalavimus nustatančiu įstatymu, dalis, procentais	–	70	100	pagal kompetenciją visos šio priedo 3–10 punktuose nurodytos institucijos
3.			Valstybės politiką elektroninės informacijos saugos (kibernetinio saugumo) srityje formuojančių ir įgyvendinančių subjektų, priklausančių nacionalinei elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo koordinavimo sistemai, dalis, procentais	–	80	100	Vidaus reikalų ministerija, Krašto apsaugos ministerija, Susisiekimo ministerija, Valstybinė duomenų apsaugos inspekcija
			Įsteigta kolegiali nuolatinė elektroninės informacijos saugos (kibernetinio saugumo) konsultacinė taryba	–	taip	taip	
4.			Atliktų elektroninės informacijos saugos srityje veikiančių pajėgumų ir jų potencialo vertinimo studijų skaičius	–	1	2	Vidaus reikalų ministerija
5.			Patvirtintos grėsmių ir pažeidžiamumų vertinimo metodikos	–	taip	taip	Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba,

Eil. Nr.	Tikslas	Uždavinys	Vertinimo kriterijus	Rodiklis 2011 metais	Rodiklis 2015 metais	Rodiklis 2019 metais	Už kriterijaus įgyvendinimą atsakinga institucija
			Atliktų grėsmių ir pažeidžiamumų vertinimų skaičius	–	4	8	Valstybinė duomenų apsaugos inspekcija
			Nevaldomų pažeidžiamumų dalis, procentais	–	20	10	
6.			Elektroninės informacijos saugos (kibernetinio saugumo) atitikties reikalavimams stebėsenos sistema stebimų informacinių sistemų dalis, procentais	0	60	100	Vidaus reikalų ministerija
7.			Informacinių sistemų valdytojų, kurių elektroninės informacijos saugos valdymo brandos lygis pakilo, dalis, procentais	–	50	100	Vidaus reikalų ministerija
8.			Valstybės institucijų, ūkio subjektų, teikiančių paslaugas valstybės institucijoms, visuomenei teikiamų viešųjų paslaugų, kurių įvertintas priklausomybės nuo kibernetinės erdvės bei informacinių ir ryšių technologijų naudojimo laipsnis, dalis, procentais	–	60	100	Vidaus reikalų ministerija, Susisiekimo ministerija
9.			Užbaigtų ikiteisminių tyrimų dėl nusikalstamų veikų, vykdomų kibernetinėje erdvėje, dalis, procentais	–	30	50	Policijos departamentas prie Vidaus reikalų ministerijos
10.			Dalyvauta tiriant kibernetinius incidentus, sukėlusius ar galėjusius sukelti krizę, procentais	–	60	90	Ministro Pirmininko tarnyba
11.		1.2. tobulinti elektroninės informacijos saugos (kibernetinio saugumo) teisinį reguliavimą	Priimtų ar pakeistų teisės aktų dalis iš tų teisės aktų, kuriuos priimti ar pakeisti nustatytas poreikis, procentais	–	80	100	pagal kompetenciją visos šio priedo 12–15 punktuose nurodytos institucijos

Eil. Nr.	Tikslas	Uždavinys	Vertinimo kriterijus	Rodiklis 2011 metais	Rodiklis 2015 metais	Rodiklis 2019 metais	Už kriterijaus įgyvendinimą atsakinga institucija
12.			Priimti esminius su elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimu susijusius reikalavimus nustatantys specialūs atitinkamą veiką ir teisinius santykius reglamentuojantys įstatymai (tarp jų Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymas)	–	taip	taip	Vidaus reikalų ministerija, Susisiekimo ministerija, Ryšių reguliavimo tarnyba
13.			Priimtų ar pakeistų įstatymo įgyvendinamųjų teisės aktų dalis iš tų teisės aktų, kuriuos priimti ar pakeisti nustatytas poreikis, procentais	–	80	100	Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija
14.			Patvirtinti reikalavimai saugaus valstybės duomenų perdavimo tinklo paslaugoms teikti	–	taip	taip	Susisiekimo ministerija, Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba
15.			Patvirtinta tapatybės nustatymo priemonių (metodų) ir paslaugų patikimumo klasifikacija (suderinta su kitų Europos Sąjungos valstybių narių), techniniai ir procedūriniai reikalavimai, akreditavimo ir naudojimo tvarka	–	taip	taip	Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba (kiek tai susiję su elektroninio parašo priežiūros institucijos funkcijomis)
16.		1.3. plėsti ir tobulinti saugią valstybės informacinę infrastruktūrą	Saugią infrastruktūrą naudojančių informacinių išteklių dalis, procentais	–	70	100	pagal kompetenciją visos šio priedo 17–21 punktuose nurodytos institucijos
17.			Patvirtinti paslaugų teikimo reikalavimai, sustiprinantys informacinės infrastruktūros paslaugas suteikiančių ūkio subjektų atsakomybę už teikiamų paslaugų saugą	–	taip	taip	Susisiekimo ministerija
18.			Lėšų, kurias informacinių sistemų valdytojai planuoja skirti informacinių sistemų saugai, ir lėšų, planuojamų skirti informacinių sistemų plėtrai ir palaikymui, santykis, procentais	–	10	15	Vidaus reikalų ministerija, Susisiekimo ministerija

Eil. Nr.	Tikslas	Uždavinys	Vertinimo kriterijus	Rodiklis 2011 metais	Rodiklis 2015 metais	Rodiklis 2019 metais	Už kriterijaus įgyvendinimą atsakinga institucija
19.			Valstybės valdymo poreikiams užtikrinti naudojamų ryšių ir informacinių sistemų rezervinių pajėgumų ir pagrindinių pajėgumų santykis, procentais	–	20	30	Susisiekimo ministerija, Vidaus reikalų ministerija
20.			Informacinių sistemų, naudojančių elektroninės valdžios informacinių išteklių kolektyvinę apsaugos nuo grėsmių iš viešųjų tinklų sistemą, dalis, procentais				Vidaus reikalų ministerija
			I kategorijos	0	80	100	
			II kategorijos	0	60	100	
			III kategorijos	0	50	100	
			IV kategorijos	0	40	100	
21.			Veikia sistema, užtikrinanti patikimą vartotojų ir informacinių išteklių tapatybės nustatymą valstybės informacinėje infrastruktūroje ir ypatingos svarbos informacinėje infrastruktūroje, taip pat teikianti elektroninio tapatybės liudijimo paslaugas	–	taip	taip	Vidaus reikalų ministerija
22.		1.4. skatinti elektroninės informacijos saugos (kibernetinio saugumo) projektų įgyvendinimą	Bendradarbiavimo tarp valstybės veiklos sričių subjektų pagrindu įgyvendintų projektų dalis nuo bendro informacinės infrastruktūros apsaugos projektų skaičiaus, procentais	–	30	50	Vidaus reikalų ministerija, Krašto apsaugos ministerija, Lietuvos mokslo ir studijų institucijų kompiuterinio tinklo LITNET (toliau – LITNET) taryba
23.			Projektų, dėl kurių pateikė pasiūlymus asociacijos, dalis, procentais	–	20	50	Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba
24.			Šalies ūkio subjektų ir mokslo įstaigų iniciatyvų (tyrimų, projektų, sprendimų ir panašiai), prie kurių įgyvendinimo prisidėjo valstybės institucijos, dalis, procentais	–	30	50	Švietimo ir mokslo ministerija, Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba, LITNET taryba

Eil. Nr.	Tikslas	Uždavinys	Vertinimo kriterijus	Rodiklis 2011 metais	Rodiklis 2015 metais	Rodiklis 2019 metais	Už kriterijaus įgyvendinimą atsakinga institucija
25.		1.5. plėtoti tarptautinį bendradarbiavimą elektroninės informacijos saugos (kibernetinio saugumo) srityje	Sričių (Europos Komisijos 2009 m. kovo 30 d. komunikate KOM (2009) 149 nurodytų uždavinių sprendimo ramsčių), kuriose bendradarbiaujama tarptautiniu lygiu, skaičius	–	3	5	pagal kompetenciją visos šio priedo 26–29 punktuose nurodytos institucijos
26.			Dalyvauta NATO, Europos Sąjungos ir Jungtinių Tautų Organizacijos renginiuose elektroninės informacijos saugos (kibernetinio saugumo) klausimais, į kuriuos buvo kviečiama, procentais	–	50	80	Ryšių reguliavimo tarnyba, Krašto apsaugos ministerija, Vidaus reikalų ministerija, Susisiekimo ministerija
27.			Į NATO kibernetinės gynybos tobulinimo centrą deleguotų atstovų skaičius	1	1	2	Krašto apsaugos ministerija
			Dalyvauta NATO kibernetinės gynybos tobulinimo centro organizuotuose renginiuose, į kuriuos buvo kviečiama, procentais	–	50	80	
28.			Dalyvauta tarptautinėse kibernetinės gynybos pratybose, į kurias buvo kviečiama, procentais	–	50	80	Ryšių reguliavimo tarnyba, Krašto apsaugos ministerija, LITNET taryba
29.			Pasirašytų bendradarbiavimo su kitų valstybių CERT centrais susitarimų skaičius	–	3	6	Ryšių reguliavimo tarnyba, Krašto apsaugos ministerija, Vidaus reikalų ministerija, LITNET taryba
30.	2. Užtikrinti ypatingos svarbos informacinės infrastruktūros efektyvų funkcionavimą		Vidutinis ypatingos svarbos informacinės infrastruktūros objektų incidentų likvidavimo laikas, valandomis	–	1	0,5	pagal kompetenciją visos šio priedo 32–40 punktuose nurodytos institucijos
31.		2.1. užtikrinti ypatingos svarbos informacinės infrastruktūros saugumą	Ypatingos svarbos informacinės infrastruktūros objektų, atitinkančių elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus, dalis, procentais	–	60	100	pagal kompetenciją visos šio priedo 32–40 punktuose nurodytos institucijos

Eil. Nr.	Tikslas	Uždavinys	Vertinimo kriterijus	Rodiklis 2011 metais	Rodiklis 2015 metais	Rodiklis 2019 metais	Už kriterijaus įgyvendinimą atsakinga institucija
32.			Identifikuotų ypatingos svarbos informacinės infrastruktūros objektų dalis, procentais	–	100	100	Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba Krašto apsaugos ministerija, LITNET taryba
			Ypatingos svarbos informacinės infrastruktūros objektų, kuriuose atlikta kritinių išteklių ir teikiamų paslaugų analizė ir veiklos sutrikdymo, sutrikus šių objektų informacinėms infrastruktūroms ar šiems objektams būtinoms išorės informacinėms infrastruktūroms, rizikos vertinimas, dalis, procentais	–	70	100	
33.			Patvirtinti saugos reikalavimai ypatingos svarbos informacinės infrastruktūros objektams	–	taip	taip	Vidaus reikalų ministerija, Krašto apsaugos ministerija, LITNET taryba
34.			Ypatingos svarbos informacinės infrastruktūros objektų, kuriuose atliktas atsparumo vertinimas, dalis, procentais	–	60	100	Vidaus reikalų ministerija
35.			Nuolat stebimų ypatingos svarbos Lietuvos elektroninių ryšių ir interneto tinklų infrastruktūros ir Lietuvos kibernetinės erdvės perimetro elementų skaičius nuo visų, procentais	–	95	99,5	Ryšių reguliavimo tarnyba, LITNET taryba
36.			Institucijų, dalyvaujančių Europos Sąjungos ypatingos svarbos infrastruktūros informacinio tinklo CIWIN (angl. *Critical Infrastructure Warning Information Network*) veikloje, skaičius	–	7	12	Ministro Pirmininko tarnyba
37.			Paskirta institucija, atsakinga už ypatingos svarbos objektų veiklos tęstinumą informacinės infrastruktūros sutrikdymo metu	–	taip	taip	Ministro Pirmininko tarnyba

Eil. Nr.	Tikslas	Uždavinys	Vertinimo kriterijus	Rodiklis 2011 metais	Rodiklis 2015 metais	Rodiklis 2019 metais	Už kriterijaus įgyvendinimą atsakinga institucija
38.			Patvirtintas valstybės gynybai skirtų institucijų ypatingos svarbos informacinės infrastruktūros objektų ir informacinių išteklių kibernetinės gynybos planas	–	taip	taip	Krašto apsaugos ministerija, Valstybės saugumo departamentas, Ryšių reguliavimo tarnyba Vidaus reikalų ministerija, Susisiekimo ministerija, Ūkio ministerija, Energetikos ministerija, Finansų ministerija
			Patvirtintas nacionalinis ypatingos svarbos informacinės infrastruktūros objektų ir valstybės informacinių išteklių kibernetinės gynybos planas	–	–	taip	
39.			Patvirtintas atsarginės infrastruktūros, reikalingos ypatingos svarbos informacinių infrastruktūrų gyvybiškumui užtikrinti, parengimo ir jos valdymo kritinių situacijų metu planas	–	taip	taip	Vidaus reikalų ministerija, Krašto apsaugos ministerija
40.			Ypatingos svarbos infrastruktūros objektų, išskyrus elektroninių ryšių tinklus, skirtus valstybės gynybai užtikrinti ir / ar reikalingus vykdant įsipareigojimus NATO ir Europos Sąjungos gynybiniams pajėgumams užtikrinti, prijungtų prie saugaus duomenų perdavimo tarp įstaigų tinklo, kurio paslaugas teikia Lietuvos Respublikos Vyriausybės paskirtas (paskirti) saugaus valstybinio duomenų perdavimo tinklo paslaugų teikėjas (teikėjai), dalis, procentais	–	70	100	Vidaus reikalų ministerija
41.	3. Užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje		Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis, procentais	–	40	60	pagal kompetenciją visos šio priedo 43–59 punktuose nurodytos institucijos

Eil. Nr.	Tikslas	Uždavinys	Vertinimo kriterijus	Rodiklis 2011 metais	Rodiklis 2015 metais	Rodiklis 2019 metais	Už kriterijaus įgyvendinimą atsakinga institucija
42.		3.1. kelti elektroninės informacijos saugos (kibernetinio saugumo) kultūrą	Lietuvos gyventojų, suvokiančių kibernetinio saugumo principus, dalis, procentais	–	60	80	pagal kompetenciją visos šio priedo 43–48 punktuose nurodytos institucijos
43.			Parengtų elektroninės informacijos saugos (kibernetinio saugumo) specialistų rengimo ir jų kvalifikacijos tobulinimo programų skaičius, vienetais	–	1	2	Švietimo ir mokslo ministerija, Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba, LITNET taryba
			Šias programas išklausiusių specialistų skaičius	–	80	200	
44.			Parengta informatikos teisės specialistų	–	20	30	Švietimo ir mokslo ministerija LITNET taryba
			Atlikta mokslinių tyrimų informatikos teisės srityje	–	10	15	
45.			Veikiančių savišvietos saugos tematika interneto svetainių skaičius	–	1	1	Vidaus reikalų ministerija, Valstybinė duomenų apsaugos inspekcija
			Svetainių naudingumą teigiamai įvertinusių lankytojų dalis, procentais	–	50	60	
46.			Organizuotų renginių, skirtų elektroninės informacijos saugos (kibernetinio saugumo) svarbos suvokimui gerinti, skaičius, vienetais	–	4	8	Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba, Švietimo ir mokslo ministerija, Valstybinė duomenų apsaugos inspekcija
47.			Naudotojų naudojamų elektroninės informacijos saugos priemonių vidutinis skaičius, vienetais	–	2	4	Vidaus reikalų ministerija, Susisiekimo ministerija, Ryšių reguliavimo tarnyba
48.			Pranešimų spaudai apie elektroninės informacijos saugos iniciatyvas skaičius	–	8	16	Ryšių reguliavimo tarnyba, Vidaus reikalų ministerija, Švietimo ir mokslo ministerija

Eil. Nr.	Tikslas	Uždavinys	Vertinimo kriterijus	Rodiklis 2011 metais	Rodiklis 2015 metais	Rodiklis 2019 metais	Už kriterijaus įgyvendinimą atsakinga institucija
49.		3.2. stiprinti Lietuvos kibernetinės erdvės saugumą	Vidutinis incidentų kibernetinėje erdvėje šalinimo laikas, valandomis	–	1	0,5	pagal kompetenciją visos šio priedo 50–52 punktuose nurodytos institucijos
50.			Veikiančių ir tarpusavyje bendradarbiaujančių CERT veiklą vykdančių reagavimo į incidentus grupių skaičius	–	5	8	Ryšių reguliavimo tarnyba, Krašto apsaugos ministerija, LITNET taryba
51.			Sukurta nacionalinė išankstinio perspėjimo apie tinklų ir informacijos saugumo pažeidžiamumus ir grėsmes sistema	–	taip	taip	Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija, LITNET taryba
52.			Neteisėtos veiklos kibernetinėje erdvėje skaitmeninių įrodymų analizės laboratorijų skaičius	–	0	1	Vidaus reikalų ministerija, Policijos departamentas prie Vidaus reikalų ministerijos, Ryšių reguliavimo tarnyba, LITNET taryba
53.		3.3. užtikrinti Lietuvos kompiuterių tinklo (virtualaus perimetro) apsaugą nuo išorinių kibernetinių atakų	Jungčių, atitinkančių elektroninės informacijos saugos reikalavimus, dalis, procentais	–	70	100	pagal kompetenciją visos šio priedo 54–56 punktuose nurodytos institucijos
54.			Sukurtos teisinės prielaidos ir patvirtinti tarptautinių tinklo jungčių įrengimo ir tolesnio jų valdymo reikalavimai, numatantys tokių tinklo jungčių operatorių atsakomybę už šių jungčių stebėjimo ir išankstinio perspėjimo, taip pat operatorių veiksmų koordinavimą, įvykus išorinei kibernetinei atakai	–	taip	taip	Susisiekimo ministerija, Ryšių reguliavimo tarnyba
55.			Paskirta institucija, atsakinga už virtualų Lietuvos kibernetinės erdvės perimetrą sudarančias jungtis valdančių operatorių priežiūrą	–	taip	taip	Susisiekimo ministerija, Ryšių reguliavimo tarnyba

Eil. Nr.	Tikslas	Uždavinys	Vertinimo kriterijus	Rodiklis 2011 metais	Rodiklis 2015 metais	Rodiklis 2019 metais	Už kriterijaus įgyvendinimą atsakinga institucija
56.			Patvirtinti Lietuvos interneto srauto mainų (ISM) nuostatai	–	taip	taip	Vidaus reikalų ministerija, Susisiekimo ministerija, Valstybinė duomenų apsaugos inspekcija
57.		3.4. stiprinti elektroninėje erdvėje teikiamų paslaugų saugumą	Elektroninėje erdvėje teikiamų paslaugų, atitinkančių elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus, dalis, procentais	–	70	100	pagal kompetenciją visos šio priedo 58–59 punktuose nurodytos institucijos
58.			Kolektyvinės kibernetinėje erdvėje teikiamų paslaugų saugos įgyvendinimo ir kontrolės sistemos saugomų ir kontroliuojamų paslaugų dalis, procentais	–	70	100	Susisiekimo ministerija, Vidaus reikalų ministerija
59.			Lietuvos gyventojų pasitikėjimo kibernetinėje erdvėje teikiamomis paslaugomis lygis, procentais	–	50	67	Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba, viešojo administravimo institucijos, teikiančios paslaugas kibernetinėje erdvėje

_____