

**2023–2030 METŲ PLĖTROS PROGRAMOS VALDYTOJOS LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTERIJOS
NACIONALINĖ KIBERNETINIO SAUGUMO PLĖTROS PROGRAMA**

**I SKYRIUS
PLĖTROS PROGRAMOS PASKIRTIS**

Valstybės veiklos sritis 6. Valstybės saugumas ir gynyba
Nacionalinio pažangos plano (toliau – NPP) pažangos uždavinių įtraukimo į 2023–2030 metų nacionalinę kibernetinio saugumo plėtros programą (toliau – Plėtros programa) logika Lietuvos Respublikos krašto apsaugos ministerija, kaip Plėtros programos valdytoja, įgyvendina 2021–2030 metų nacionalinio pažangos plano, patvirtinto Lietuvos Respublikos Vyriausybės 2020 m. rugsėjo 9 d. nutarimu Nr. 998 „Dėl 2021–2030 metų nacionalinio pažangos plano patvirtinimo“, dešimtojo strateginio tikslo „Stiprinti nacionalinį saugumą“ 10.5 uždavinį „Stiprinti kibernetinį saugumą ir gynybą“.
Plėtros programoje nustatomos civilinio sektoriaus kibernetiniam saugumui stiprinti reikalingos priemonės.
NPP pažangos uždavinys, kodas ir pavadinimas 10.5 uždavinys „Stiprinti kibernetinį saugumą ir gynybą“
NPP pažangos uždavinio poveikio rodiklis ir (ar) NPP strateginio tikslo poveikio rodiklis NPP 10.5 uždavinio rodiklis: 10.5.1. Kibernetinio saugumo indeksas, Lietuvos įvertinimas balais. Pradinė rodiklio reikšmė (2020 m.) – 97,93 balo; tarpinė rodiklio reikšmė (2025 m.) – 98,25 balo; galutinė rodiklio reikšmė (2030 m.) – 98,5 balo. Pasaulinis kibernetinio saugumo indeksas (toliau – KSI) yra kompleksinis rodiklis, kuris skaičiuojamas pagal kintančias skaičiavimo metodikas ir pagal kurį lyginamos įvairių pasaulio valstybių finansuojamos pastangos bei pažanga kibernetinio saugumo srityje atitinkamais metais (t. y. neatsižvelgiant į bazinės datos lyginamuosius rodiklius). Lietuva KSI 2020 m. užėmė 6 poziciją pasaulyje ir 4 poziciją Europoje. Maksimalų vertinimą Lietuva surinko teisinio reguliavimo bei švietimo ir edukacijos srityse (20 taškų iš 20 galimų). Techninių (19,54 taško iš 20 galimų) ir organizacinių (18,98 taško iš 20 galimų) priemonių bei bendradarbiavimo (19,41 taško iš 20 galimų) kryptis reikia stiprinti. Siekiant išlaikyti ir gerinti užimamas pozicijas KSI, būtina šalinti Plėtros programoje nurodytas esamų problemų priežastis, siekti pažangos KSI vertinamose srityse ir skirti pakankamą finansavimą. Lietuvos tikslas – šalinant Plėtros programoje nurodytas problemų priežastis išlaikyti ir (ar) pagerinti aukštą Lietuvos KSI. Visas Plėtros programoje nurodytas problemos priežastis galima susieti su pažanga 5 (penkiose) KSI vertinamose srityse:

- teisinės priemonės – 1.1, 1.2;
- organizacinės priemonės – 1.3;
- techninės priemonės – 1.4, 2.1;
- švietimo ir gebėjimų plėtojimo priemonės – 1.5, 1.6, 2.2, 3;
- bendradarbiavimo priemonės – 4.

Problema – dėl pasikeitusių kibernetinių grėsmių pobūdžio ir augančio jų masto mažėjantis šalies kibernetinis atsparumas.

Spręstinės problemos priežastys (prioriteto tvarka):

1. Esamas kibernetinio saugumo modelis netinkamas augančiai kibernetinio saugumo sričiai:
 - 1.1. plečiantis kibernetinio saugumo taikymo sričiai trūksta kibernetinio saugumo politikos įgyvendinimo procese dalyvaujančių suinteresuotųjų subjektų;
 - 1.2. nesukurti kibernetinio saugumo reikalavimų atnaujinimo metodai;
 - 1.3. skirtingai taikomos kibernetinio atsparumo priemonės viešajame sektoriuje;
 - 1.4. kibernetinio saugumo, atsparumo ir grėsmės lygiui vertinti trūksta kibernetinio saugumo stebėsenos duomenų;
 - 1.5. nenuoseklus valstybės institucijų personalo švietimas ir edukacija kibernetinio saugumo klausimais;
 - 1.6. trūksta kibernetinio saugumo specialistų.
2. Nusikalstamų veikų elektroninėje erdvėje tyrimo pajėgumai neatitinka nusikalstamų veikų sudėtingumo:
 - 2.1. nevystoma elektroninių nusikaltimų tyrimo infrastruktūra;
 - 2.2. mažai dėmesio skiriama elektroninių nusikaltimų tyrėjų kompetencijoms didinti.
3. Žemas visuomenės ir smulkaus bei vidutinio verslo žinių kibernetinio saugumo srityje lygis ir praktiniai gebėjimai jas pritaikyti.
4. Nenustatytos viešojo ir privataus sektoriaus bendradarbiavimo kryptys.

Pažangos priemonė, kuria sprendžiama problema:

06-007-10-05-07 „Stiprinti kibernetinį atsparumą“ (šalinamos 1–4 priežastys).

Pažangos priemonės, numatytos kitose plėtros programose:

Viešojo saugumo stiprinimo ir plėtros programos pažangos priemonė Nr. 07-011-10-07-01/07-019-10-07-01 „Sudaryti prielaidas veiksmingai nusikaltimų prevencijai ir kontrolei bei terorizmo grėsmių mažinimui“ (šalinama 2 priežastis).

Pastaba. Kibernetinio saugumo indekso reikšmė pateikta ITU *Global Cybersecurity Index*, 2020, <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>.

II SKYRIUS FINANSAVIMO PLANAS

NPP pažangos uždavinys	Finansinių projekcijų dalys ir kitos lėšos tūkst. Eur	Finansavimo šaltiniai	NPP finansavimo sąlygų tenkinimas
1	2	3	4
	40 150	Ekonomikos gaivinimo ir atsparumo didinimo priemonės lėšos	

10.5 Stiprinti kibernetinį saugumą ir gynybą	8 432	Valstybės biudžeto lėšos, skirtos Europos Sąjungos fondų lėšomis netinkamam finansuoti PVM apmokėti	NPP dešimtojo strateginio tikslo finansavimui keliamos sąlygos nėra taikomos.
	1 868	Kitos tarptautinės paramos lėšos (2021–2027 m. Skaitmeninės Europos programos lėšos)	
	1 868	2021–2027 m. Skaitmeninės Europos programos bendrojo finansavimo lėšos	
	Iš viso 52 318		

III SKYRIUS PRIEMONIŲ RINKINYS

Priemonės kodas	Pažangos priemonė ir regioninė pažangos priemonė (toliau kartu – priemonė)	NPP pažangos uždavinys	Kiti NPP pažangos uždaviniai	Būtiniosios sąlygos	Dalyvaujančios institucijos	Priemonės stebėsenos rodiklio pavadinimas	Priemonės stebėsenos rodiklio reikšmės		Priemonės papildomas požymis
							2022	2030	
1	2	3	4	5	6	7	8	9	10
06-007-10-05-07	Stiprinti kibernetinį atsparumą	10.5 Stiprinti kibernetinį saugumą ir gynybą	-	1. Nacionalinio koordinavimo centro, kuris užtikrins kibernetinio saugumo inovacijų skatinimo funkcijų, numatytų Reglamente (ES) 2021/887 , įgyvendinimą, sukūrimas. 2. Kibernetinio saugumo modelio atnaujinimas, atsižvelgiant į Direktyvoje (ES) 2022/2555 numatytus reikalavimus.	Vidaus reikalų ministerija	Ištirtų kritinių kibernetinių incidentų dalis (proc.).	50	100	HP (darnaus vystymosi, inovatyvumo), Vyriausybės programos nuostatų įgyvendinimo planas
						Atitiktį kibernetinio saugumo organizaciniais ir techniniams reikalavimams deklaravusių kibernetinio saugumo subjektų, valdančių ir (arba) tvarkančių valstybės informacinius išteklius, ypatingos svarbos informacinę infrastruktūrą, dalis (proc.).	30	90	
						Dėl atitikties kibernetinio saugumo organizaciniais ir techniniams reikalavimams įvertintų kibernetinio saugumo subjektų, valdančių ir (arba) tvarkančių ypatingos svarbos informacinę infrastruktūrą, dalis (proc.).	20	80	

						Visuomenės narių, patikrinančių interneto svetainės saugumą prieš teikiant joje savo asmens duomenis, dalis (proc.).	23,3 (2021)	40	
						Kibernetinio saugumo subjektų vadovų, sėkmingai išlaikiusių kibernetinio saugumo žinių ir kompetencijų įvertinimo testus, dalis (proc.).	n/a	80	

Pastaba. Aštuonioliktosios Lietuvos Respublikos Vyriausybės programos nuostatų įgyvendinimo planas, patvirtintas Lietuvos Respublikos Vyriausybės 2021 m. kovo 10 d. nutarimu Nr. 155 „Dėl Aštuonioliktosios Lietuvos Respublikos Vyriausybės programos nuostatų įgyvendinimo plano patvirtinimo“.
