NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
PRIE KRAŠTO APSAUGOS MINISTERIJOS

TVIRTINU
Lietuvos Respublikos
krašto apsaugos ministras

Robertas Kaunas

2026-ŲJŲ METŲ VEIKLOS PLANAS

2026-03-04 Nr. (1.8 E) 10K-70
Vilnius

VEIKLOS VYKDYMAS

Eil. Nr.	Programos, programos priemonės, veiksmo pavadinimas	Atsakingi vykdytojai	Terminas/ planuojami asignavimai priemonei	Įvykdymo data	Įvykdymo procentas	Veiksmo būsena	VPNĮP, NPP, KAS SPP, NKSPP kodas; KAM plano, PPBS plano veiksmo eil. Nr.
1	2	3	4	5	6	7	8
NKSC misija – įkvėpti ir įgalinti Lietuvos žmones ir organizacijas apsaugoti savo informaciją, paslaugas ir turtą nuo kibernetinių grėsmių.							
NKSC vizija – Lietuva yra atspari kibernetinėms grėsmėms.							
Ekonomikos gaivinimo ir atsparumo didinimo priemonė (RRF projektai)		**NKSC**	**4 886,9 tūkst. Eur (RRF lėšos)**	-	-	-	-
Programa: Krašto apsaugos sistemos veiklos parama 06-007							
5 uždavinys „Stiprinti kibernetinį saugumą ir gynybą“ (06-007-10-05)							
5 uždavinio 7 priemonė „Stiprinti kibernetinį atsparumą“ (06-007-10-05-07)		**NKSC**	**135 tūkst. Eur**	-	-	-	-
Priemonė įgyvendinama 4.2 papunktyje nurodytu veiksmu, kurio rezultatas „Įgyvendintas Cyber Up projektas“							
1 uždavinys „Plėtoti KAS materialinę bazę, organizuoti informacinį aprūpinimą, įgyvendinti finansų valdymo politiką ir užtikrinti atstovavimą Lietuvos atstovybėse ir tarptautinėse organizacijose“ (06-007-11-01)		**NKSC**					
1 uždavinio 1 priemonė „Užtikrinti KAS materialinės bazės funkcionavimą, informacinį aprūpinimą, piniginių ir materialinių išteklių naudojimą ir organizuoti centralizuotus KAS pirkimus“ (06-007-11-01-01)		**NKSC**	**15 tūkst. Eur**	-	-	-	-
1 uždavinio 4 priemonė „Pervesti įmokas ir dotacijas, mokamas tarptautinėms organizacijoms (institucijoms), įgyvendinamoms tarptautinių organizacijų ir užsienio valstybių programoms ir projektams, taip pat subsidijas privalomąją pradinę karo tarnybą atlikusių karo prievolininkų darbo užmokesčiui“ (06-007-11-01-04)		**NKSC**	**1,5 tūkst. Eur**	-	-	-	-
4 uždavinys „Užtikrinti valstybės kibernetinio saugumo politikos įgyvendinimą ir ryšių ir informacinių sistemų (RIS) plėtojimą“ (06-007-11-04)		**NKSC**					
4 uždavinio 1 priemonė „Vykdyti kibernetinio saugumo veiklas ir teikti elektroninių ryšių paslaugas“ (06-007-11-04-01)		**NKSC**	**10 769,5 tūkst. Eur**	-	-	-	-
Priemonė įgyvendinama visais veiksmais, išskyrus 4.2 papunktyje nurodytu veiksmu, kurio rezultatas „Įgyvendintas Cyber Up projektas“							
1.	**Strateginė kryptis: Ugdyti klientų brandą ir kompetencijas**						

1.1.	**Įgyvendinti RRF1 projektą „Nacionalinės kibernetinio saugumo stebėsenos sistemos sukūrimas"**	ITD	Gegužė				NKSPP
	Laukiamas rezultatas: pasiekti visi projekto plane apibrėžti rezultatai, kurie detaliai stebimi projektų portfelio švieslentėje						
1.2.	**Įgyvendinti RRF3 projektą „Nusikalstamų veikų elektroninėje erdvėje tyrimui ir mokymams skirtos laboratorijos sukūrimas ir įveiklinimas"**	ITD	Balandis				NKSPP
	Laukiamas rezultatas: pasiekti visi projekto plane apibrėžti rezultatai, kurie detaliai stebimi projektų portfelio švieslentėje						
1.3.	**Stebėti kibernetinio saugumo subjektų atitiktį kibernetinio saugumo reikalavimams bei rizikų valdymą**	KAVD	Balandis				VPNĮP 4.3.16
	Laukiamas rezultatas:						
1.3.1.	Parengti ir patvirtinti planinį esminių kibernetinio saugumo subjektų patikrinimų planą	KAVD	Kovas				
1.3.2.	Papildyti KSS registrą subjektais pagal specialiuosius kriterijus	KAVD	Balandis				
1.4.	**Ugdyti ir įgalinti KSS pasitikrinti praktinius kibernetinio saugumo įgūdžius**	PKSD	Gruodis				
	Laukiamas rezultatas:						
1.4.1.	Parengti ir patvirtinti metinį KSS pratybų planą	PKSD	Vasaris				
1.4.2.	Surengti ne mažiau kaip 3 mokymų renginius mokymų klasėse	PKSD	Gruodis				
1.5.	**Vykdyti Nacionalinės komunikacijų apsaugos priežiūros tarnybos, Saugumo priežiūros institucijos, Nacionalinės šifrų paskirstymo tarnybos ir Lietuvos Respublikos įslaptintos informacijos, užsienio valstybių, Europos Sąjungos ir tarptautinių organizacijų Lietuvos Respublikai perduotos įslaptintos informacijos, apdorojamos ar perduodamos ĮIRIS, TEMPEST tarnybos funkcijas**	KAVD	Birželis				
	Laukiamas rezultatas:						
1.5.1.	Parengti ir patvirtinti 2026-2028 m. ĮIRIS patikrinimų planą	KAVD	Sausis				
1.5.2.	Parengti LR Vyriausybės 2019 m. nutarimo Nr. 40-1 „Dėl įslaptintos informacijos ryšių ir informacinių sistemų apsaugos įgyvendinimo“ keitimo teisės aktų projektus pagal naujausias NATO ir ES direktyvas ir suderinti su suinteresuotomis šalimis	KAVD	Birželis				
1.6.	**Vykdyti Nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas**	KAVD	Rugsėjis				
	Laukiamas rezultatas: Parengti ir patvirtinti pasiruošimo ES Nacionalinių kibernetinio sertifikavimo institucijų tarpusavio peržiūrai (2028 m.) veiksmų planą						
2.	**Strateginė kryptis: Teikti kokybišką pagalbą valdant kibernetinius incidentus**						
2.1.	**Didinti NKSC kibernetinio saugumo paslaugų kokybę ir prieinamumą**	KSOVD	Gruodis				
	Laukiamas rezultatas:						
2.1.1.	Parengti ir patvirtinti NKSC atitkties SIM3 Advanced lygiui planą	KSOVD	Vasaris				
2.1.2.	Sertifikuoti / akredituoti KAM SOC	KSOVD	Birželis				
2.1.3.	Ištestuoti SOP nacionalines CRRT	KGVD	Birželis				
2.1.4.	Atnaujinti ir patvirtinti NKSC paslaugų sąrašą pagal FIRST metodiką	KSOVD	Birželis				

2.1.5.	Atnaujinti ir patvirtinti techninių kibernetinio saugumo priemonių, diegiamų KSS infrastruktūroje koncepciją (tinklo srautų stebėjimo sensoriai, agentai ir kt.)	ITD	Spalis				
2.1.6.	Parengti ir patvirtinti pažangių nuolatinių grėsmių (APT) identifikavimo procesą	KSOVD	Spalis				
2.1.7.	Gauti SIM3 Advanced sertifikatą visa apimtimi	KSOVD	Gruodis				
2.2.	**Pasirengti užtikrinti veiklos tęstinumą krizų ir ekstremaliųjų situacijų metu**	RVS	Spalis				
	Laukiamas rezultatas:						
2.2.1.	Išplėsti KAM SOC pajėgumus ir paslaugas	KSOVD	Birželis				
2.2.2.	Atnaujinti ir patvirtinti NKSC Mobilizacijos planą	RVS	Rugsėjis				
2.2.3.	Užtikrinti IT veiklos atstatymą (angl. Disaster Recovery), įdiegiant duomenų ir paslaugų replikavimą tarp valstybinio duomenų centro Vilniuje ir Kaune esančios serverinės	ITD	Rugsėjis				
2.2.4.	Parengti, patvirtinti ir ištestuoti NKSC Kibernetinių krizių valdymo planą	RVS	Plano tvirtinimas - Balandis, testavimas - Spalis				
3.	**Teikti kokybišką informaciją apie galimas grėsmes ir pažeidžiamumus**						
3.1.	**Vystyti teikiamas kibernetinių grėsmių analizės paslaugas**	KGVD	Gruodis				
	Laukiamas rezultatas:						
3.1.1.	Parengti Lietuvos kibernetinių grėsmių metinį žemėlapį	KGVD	Balandis				
3.1.2.	Pradėti rengti sektorines ataskaitas ne mažiau nei 2 naujiems esminiams sektoriams	KGVD	Birželis				
3.1.3.	Patvirtinti tyrimų pajėgumo (įskaitant techninę įrangą ir ekspertų kompetenciją) aprašą ir paslaugų partneriams sąrašą	KGVD	Birželis				
3.1.4.	Parengti ir patvirtinti prioritetinių-kompleksinių tyrimų sąrašą	KGVD	Birželis				
3.1.5.	Automatizuoti sektorinių ataskaitų siuntimą	KGVD	Gruodis				
3.2.	**Įgyvendinti Tarptautinio kibernetinių grėsmių analizės (ang. *International Cyber Threat Analysis Hub*) projekto veiklas**	KGVD	Birželis				
	Laukiamas rezultatas: pasirašyti Supratimo memorandumą (MoU) dėl Tarptautinio kibernetinių grėsmių analizės pajėgumo (ang. International Cyber Threat Analysis Hub)	KGVD	Birželis				
3.3.	**Įgyvendinti Nordic-Baltic Cyber Consortium (NBCC) projektą**	KGVD	Gruodis (projekto pabaiga 2029 m.)				
	Laukiamas rezultatas: pasiekti visi projekto plane apibrėžti rezultatai, kurie detaliai stebimi projektų portfelio švieslentėje	KGVD	Gruodis				
3.4.	**Ieškoti ir koordinuoti pažeidžiamumus**	KSOVD	Spalis				
	Laukiamas rezultatas:						

3.4.1.	Parengti KSĮ keitimo siūlymus, susijusius su spragų paieška ir atskleidimu (nacionalinė spragų paieškos ir atskleidimo programa), ir suderinti juos su suinteresuotomis šalimis	KSOVD	Balandis				
3.4.2.	Įvertinti galimybes vykdyti pažeidžiamumų paiešką ĮIRIS	KSOVD	Spalis				
3.5.	**Pritraukti ES finansavimą kibernetinių grėsmių ir pažeidžiamumų analizės pajėgumams vystyti**	VES	Gegužė				
	Laukiamas rezultatas: Pateiktos ne mažiau kaip 2 paraiškos Skaitmeninės Europos programos (angl. *Digital Europe Programme (DIGITAL*) kvietimams	VES	Gegužė				
4.	**Strateginė kryptis: Didinti kibernetinio saugumo prieinamumą**						
4.1.	**Įgyvendinti RRF2 projektą "Nacionalinės SOC/CSIRT modulinės sistemos sukūrimas"**	ITD	Gegužė				NKSPP, VPNĮP 4.3.16
	Laukiamas rezultatas: pasiekti visi projekto plane apibrėžti rezultatai, kurie detaliai stebimi projektų portfelio švieslentėje						
4.2.	**Kurti dinamišką ir aktyvią Lietuvos kibernetinio saugumo bendruomenę (vykdyti Nacionalinio koordinavimo centro funkcijas)**	VES	Balandis				NKSPP, VPNĮP 4.3.17
	Laukiamas rezultatas:						
4.2.1.	Parengti ir patvirtinti projekto „Cyber Lietuva“ įgyvendinimo veiksmų planą	VES	Kovas				
4.2.2.	Pasiekti visi projekto Cyber Up (5 uždavinio 7 priemonės "Stiprinti kibernetinį atsparumą" (06-007-10-05-07) plane apibrėžti rezultatai, kurie detaliai stebimi projektų portfelio švieslentėje	VES	Balandis				
4.3.	**Pasiruošti kibernetinio saugumo renginių organizavimui ir pirmininkavimui Lietuvos pirmininkavimo ES Tarybai 2027 m. metu**	PKSD	Birželis				
	Laukiamas rezultatas: parengti ir patvirtinti NKSC pasirengimo įgyvendinti 2027 m. I pusmečio renginių, susijusių su pirmininkavimo laikotarpiu, planą						
4.4.	**Įvairiais būdais ir priemonėmis gilinti įvairių visuomenės grupių žinias kibernetinio saugumo srityje**	PKSD, ITD	Lapkritis				
	Laukiamas rezultatas:						
4.4.1.	Parengti ir patvirtinti mokymų klasių įveiklinimo planą	PKSD	Kovas				
4.4.2.	Sukurti DNS užkardos pagrindu veikiantį saugaus interneto sprendimą (Protective DNS / Family Shield) viešosioms įstaigoms (mokyklos, ligoninės, traukiniai ir pan.)	ITD	Liepa				
4.4.3.	Parengti CTF užduočių platformą savarankiškam mokymuisi	PKSD	Rugsėjis				
4.4.4.	Įkurti pramoninių technologijų kibernetinio saugumo mokymų klasę (OT Cyber Range)	ITD	Rugsėjis				
4.4.5.	Įgyvendinti viešinimo kampaniją "Spalis - kibernetinio saugumo mėnuo"	PKSD	Lapkritis				
4.5.	**Įgyvendinti techninius kibernetinio saugumo didinimo sprendimus**	ITD	Gruodis				
	Laukiamas rezultatas: Įdiegti pokalbių robotą NKSC svetainėje skirtą išorinių naudotojų užklausų apdorojimui						
5.	**Strateginė kryptis: Puoselėti NKSC kaip geidžiamiausią vietą dirbti**						

5.1.	**Didinti NKSC veiklos efektyvumą**						
	Laukiamas rezultatas:						
5.1.1.	Įgyvendinti OVD struktūrinius pokyčius	OVD	Balandis				
5.1.2.	Parengti naują NKSC interneto svetainių koncepciją	PKSD	Gegužė				
5.1.3.	Sukurti Veiklos efektyvinimo idėjų registrą	VES	Birželis				
5.1.4.	Sukurti Riboto naudojimo tinklo DEIVIS infrastruktūroje pilotinį projektą ir pasiūlyti KSITPG galimą įgyvendinimo sprendimą	ITD	Liepa				
5.1.5.	Parengti metinio veiklos plano rodiklių švieslentę	OVD	Liepa				
5.1.6.	Parengti NKSC procesų schemas ir aprašymus, nustatyti procesų rodiklius	VES	Rugsėjis				
5.1.7.	Skaitmenizuoti žmogiškųjų išteklių valdymo funkcijas	OVD	Rugsėjis				
5.1.8.	Sukurti ISO sertifikatų valdymo praktikų sistemą	VES	Lapkritis				
5.1.9.	Planuoti 2027-2029 m. asignavimų poreikį lėšas susiejant su veiklomis	OVD	Gruodis				
5.2.	**Valdyti žmogiškuosius išteklius skatinant profesionalumą**						
	Laukiamas rezultatas:						
5.2.1.	Sukurti NKSC Naujoko dienos koncepciją	PKSD	Kovas				
5.2.2.	Sukurti kompetencijų matricą ir įvertinti darbuotojų kompetencijų lygį	OVD	Spalis				
5.2.3.	Įdiegti ir įveiklinti bandomąjį vidinį LLM darbui su KAM SOC naudojamu Elasticsearch	ITD	Gruodis				
5.3.	**Gerinti darbo sąlygų, aplinkos ir naudojamų technologijų kokybę**	ITD	Rugsėjis				
	Laukiamas rezultatas: Sukurti vidinės NKSC žinių bazės agentą						

STEBĖSENOS RODIKLIŲ SUVESTINĖ

Programos, tikslo, uždavinio, priemonės, rodiklio kodas	Programos, veiklos tikslo, uždavinio, priemonės, stebėsenos rodiklio pavadinimas	Rodiklių reikšmės									VPNĮP, NDĮP, NPP, KAS SPP, rodiklio kodas
		Faktinė reikšmė		Siektina reikšmė	Faktinė reikšmė	Įvykdymo procentas	Siektina reikšmė				
		2024 metais	2025 metais	2026 metais	2026 metais	2026 metais	2027 metais	2028 metais	2029 metais	2030 metais	
1	2	3	4	5	6	7	8	9	10	11	12
006-007	**Programa:** Krašto apsaugos sistemos veiklos parama										
06-007-10-05-07	**Priemonė:** Stiprinti kibernetinį atsparumą										
	NKSC registruotų didelio poveikio kibernetinių incidentų	18	19	–	–	–	–	–	–	–	NPP (17)

R-06-007-10-05-07-01	skaičius, vnt.										
	Rezultatas:										
R-06-007-10-05-07-02	NKSC ištirtų didelio poveikio kibernetinių incidentų dalis, proc.*	-									NPP (18)
		67	100	80	-	-	90	90	95	100	NKSPP
	Rezultatas:										
R-06-007-10-05-07-03	Dėl atitikties kibernetinio saugumo organizaciniams ir techniniams reikalavimams įvertintų kibernetinio saugumo subjektų, valdančių ir (arba) tvarkančių ypatingos svarbos informacinę infrastruktūrą, dalis, proc.	35	44	53	-	-	58	65	80	90	NKSPP
	Rezultatas:										
R-06-007-10-05-07-05	Kibernetinio saugumo subjektų vadovų, sėkmingai išlaikiusių kibernetinio saugumo žinių ir kompetencijų įvertinimo testus, dalis, proc.	Didėjimas									NPP (20)
		ND	22	20	-	-	50	70	80	90	NKSPP
	Rezultatas:										
R-06-007-10-05-07-06	Kibernetinio saugumo stebėsenos sistemos skaitmeninio sprendimo įdiegimas, proc.	ND	55	100	-	-	-	-	-	-	-
	Rezultatas:										
R-06-007-10-05-07-07	Kibernetinio saugumo subjektų darbuotojų, sėkmingai išlaikiusių kibernetinio saugumo higienos kursą dalis, proc.	ND	ND	Didėjimas							NPP (21)
	Rezultatas:										
06-007-11-04	**Uždavinys:** Užtikrinti valstybės kibernetinio saugumo politikos įgyvendinimą ir ryšių ir informacinių sistemų (RIS) plėtojimą										
	Kibernetinio saugumo rizikų valdymo priemones taikančių ir organizacinius techninius	Didėjimas									NPP (22)

E-06-007-11-04-01	reikalavimus įgyvendinančių kibernetinio saugumo subjektų dalis, proc. **	25	15	60	-	-	75	80	95	100	NKSPP
	Rezultatas:										
06-007-11-04-01	**Priemonė:** Vykdyti kibernetinio saugumo veiklas ir teikti elektroninių ryšių paslaugas (NPP 10.5)										
R-06-007-11-04-01-01	Prisijungusių prie Kibernetinio saugumo informacinės sistemos kibernetinio saugumo subjektų dalis, proc.	ND	66	100	-	-	-	-	-	-	-
	Rezultatas:										
R-06-007-11-04-01-02	Kibernetinio saugumo kompetencijos bendruomenės, sudaromos Reglamento (ES) 2021/887 8 straipsnio pagrindu, narių skaičius, vnt.	0	30	45	-	-	60	70	80	90	-
	Rezultatas:										
-	Kibernetinio saugumo švietimo veiklose dalyvavusių asmenų skaičius, vnt.	-	-	1 100	-	-	1 200	1 200	1 300	1 500	NDĮP
	Rezultatas:										

* Atitinka NKSPP rodiklį „Ištirtų kritinių kibernetinių incidentų dalis, proc.“.

** Atitinka NKSPP rodiklį „Atitiktį kibernetinio saugumo organizaciniams ir techniniams reikalavimams deklaravusių kibernetinio saugumo subjektų, valdančių ir (arba) tvarkančių valstybės informacinius išteklius, ypatingos svarbos informacinę infrastruktūrą, dalis, proc.“

DEIVIS – Duomenų efektyvaus ir integruoto valdymo informacinė sistema;
DNS – Domenų vardų sistema (angl. *Domain Name System*);
ES – Europos Sąjunga;
ITD – NKSC Informacinių technologijų departamentas;
ĮIRIS – įslaptintos informacijos ryšių ir informacinė sistema;
CSIRT – reagavimo į kompiuterinius incidentus grupė;
KAM – Krašto apsaugos ministerija;
KAM SOC – NKSC KSOVD Kibernetinio saugumo skyrius;
KAS – krašto apsaugos sistema;
KAS SPP – Krašto apsaugos sistemos plėtros programa;
KAVD – NKSC Kibernetinio atsparumo vystymo departamentas;
KGVD – NKSC Kibernetinių grėsmių vystymo departamentas;
KPAP – kriptografinių priemonių administravimo punktas;
KSIS – Kibernetinio saugumo informacinė sistema;
KSOVD – NKSC Kibernetinio saugumo operacijų valdymo departamentas;
KSS – kibernetinio saugumo subjektas;

LRV – Lietuvos Respublikos Vyriausybė;
LMM – Didelio masto kalbos modelis (angl. *Large Language Model*)
LMS – Mokymosi valdymo sistema *(angl. Learning Management System*)
ND – nėra duomenų;
NKSC – Nacionalinis kibernetinio saugumo centras prie KAM;
NKSPP – Nacionalinė kibernetinio saugumo plėtros programa;
NPP – Nacionalinis pažangos planas;
OVD – NKSC Organizacinio vystymo departamentas;
PKSD – NKSC Partnerysčių ir kompetencijų stiprinimo departamentas;
RIS – ryšių informacinės sistemos;
RVS – NKSC Rizikų valdymo skyrius;
RRF – Ekonomikos gaivinimo ir atsparumo didinimo priemonė (angl. *Recovery and Resilience Facility*);
SOC – Kibernetinio saugumo operacijų centras;
SVP – Lietuvos Respublikos krašto apsaugos ministro valdymo sričių strateginis veiklos planas;
TEMPEST – apsauga nuo elektromagnetinės spinduliuotės;
VES – NKSC Veiklos efektyvumo skyrius;
VPNĮP – Vyriausybės programos nuostatų įgyvendinimo planas.

Direktorius Antanas Aleknavičius

_____