PATVIRTINTA
Lietuvos Respublikos valstybės kontrolieriaus
2021 m. birželio 7 d. įsakymu Nr. VE-85
(Lietuvos Respublikos valstybės kontrolieriaus
2026 m. kovo 19 d. įsakymo Nr. VE-25 redakcija)

INFORMACINIŲ TECHNOLOGIJŲ DEPARTAMENTO INFORMACINIŲ TECHNOLOGIJŲ ANALITIKO PAREIGYBĖS APRAŠYMAS	
1. Tiesioginis vadovas	Informacinių technologijų departamento vadovas
2. Pareigybės lygis	11
3. Pareigybės kodas pagal profesijų klasifikatorių	251101
4. Pareigybės tipas	specialistas
5. Pareigybės paskirtis	užtikrinti Valstybės kontrolės informacinių technologijų infrastruktūros ir informacinių sistemų kibernetinį saugumą, administruoti tinklo ir serverių sistemas bei analizuoti ir valdyti informacinių technologijų saugumo incidentus.
6. Specialieji pareigybei keliami reikalavimai:	
6.1. Išsilavinimas	aukštasis universitetinis išsilavinimas (ne žemesnis kaip bakalauro kvalifikacinis laipsnis) arba jam lygiavertė aukštojo mokslo kvalifikacija.
6.2. Kompiuterinis raštingumas	geri darbo *Microsoft Office* programiniu paketu įgūdžiai.
6.3. Profesinės patirties reikalavimas	ne mažesnė kaip 2 metų darbo patirtis informacinių technologijų srityje.
6.4. Užsienio kalbos reikalavimas	kalba – anglų; kalbos mokėjimo lygis – B1.
6.5. Žinios ir įgūdžiai	6.5.1. išmanyti Lietuvos Respublikos teisės aktus, reglamentuojančius informacinių technologijų ir kibernetinio saugumo sritį; 6.5.2. išmanyti informacinių technologijų infrastruktūros ir informacinių sistemų saugumo principus, įskaitant kibernetinių įvykių ir incidentų nustatymo, analizės ir valdymo pagrindus; **(2026-04-23 VE-46)** 6.5.3. išmanyti kompiuterinių tinklų, darbo vietų ir serverių saugumo valdymą; 6.5.4. išmanyti *Windows* ir *Linux* operacinių sistemų administravimo ir saugumo principus; 6.5.5. išmanyti *Microsoft 365* aplinkos saugumo valdymą; 6.5.6. išmanyti kompiuterinių tinklų ir interneto paslaugų saugumo principus; 6.5.7. išmanyti reliacinių duomenų bazių valdymo sistemų saugumo principus; 6.5.8. mokėti administruoti kompiuterinius tinklus, *Linux* operacines sistemas ir MySQL duomenų bazių valdymo sistemas; 6.5.9. gebėti diegti, konfigūruoti ir administruoti

	informacinių technologijų saugumo sprendimus; 6.5.10. gebėti atlikti informacinių technologijų infrastruktūros saugumo skenavimus ir analizuoti jų rezultatus; 6.5.11. gebėti analizuoti, sisteminti ir apibendrinti informaciją, įskaitant kibernetinio saugumo įvykių, incidentų ir grėsmių analizę; **(2026-04-23 VE-46)** 6.5.12. išmanyti informacinių technologijų paslaugų valdymo principus (ITIL).
6.6. Kiti reikalavimai	atitikti teisės aktuose nustatytus reikalavimus, būtinus išduodant leidimą dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žyma „Slaptai“.

7. Funkcijos: **(2026-04-23 VE-46)**

7.1. Dalyvauja rengiant informacinių technologijų ir kibernetinio saugumo dokumentus, planus ir kitus su saugumu susijusius dokumentus.
7.2. Analizuoja Valstybės kontrolės informacinių technologijų infrastruktūros ir informacinių sistemų saugumą, teikia pasiūlymus dėl jo gerinimo.
7.3. Administruoja Valstybės kontrolės kompiuterinius tinklus ir užtikrina jų saugų veikimą.
7.4. Administruoja „Linux“ operacines sistemas ir užtikrina jų saugų veikimą.
7.5. Administruoja duomenų bazių valdymo sistemas ir užtikrina jų saugumą.
7.6. Administruoja saugumo operacijų centre naudojamą programinę ir techninę įrangą.
7.7. Administruoja informacinių technologijų saugumo informacines sistemas ir antivirusinę programinę įrangą.
7.8. Vykdo informacijos, perduodamos Valstybės kontrolės kompiuteriniais tinklais, technologinę ir kibernetinę apsaugą.
7.9. Atlieka informacinių technologijų infrastruktūros saugumo skenavimus ir analizuoja jų rezultatus.
7.10. Vykdo informacinių technologijų infrastruktūros ir informacinių sistemų kibernetinio saugumo įvykių stebėseną.
7.11. Renka, analizuoja ir vertina informaciją apie kibernetines grėsmes, saugumo įvykius ir galimus pažeidžiamumus.
7.12. Analizuoja kibernetinio saugumo įvykius, nustato galimas grėsmes, sutrikimus ir neleistiną veiklą informacinėse sistemose ir tinkluose.
7.13. Klasifikuoja ir skirsto kibernetinio saugumo įvykius ir incidentus pagal jų reikšmingumą ir poveikį.
7.14. Vykdo kibernetinių incidentų pirminį tyrimą, nustato jų priežastis, mastą ir aplinkybes.
7.15. Renka, kaupia ir dokumentuoja su kibernetiniais incidentais susijusią informaciją.
7.16. Dalyvauja kibernetinių incidentų valdyme, bendradarbiauja su kitais padaliniais ir Nacionaliniu kibernetinio saugumo centru.
7.17. Rengia ataskaitas apie kibernetinius įvykius, incidentus ir jų valdymo rezultatus.
7.18. Atlieka informacinių technologijų infrastruktūros ir informacinių sistemų pažeidžiamumų vertinimą.
7.19. Teikia siūlymus ir rekomendacijas dėl kibernetinio saugumo stiprinimo, rizikų mažinimo ir nustatytų trūkumų šalinimo.
7.20. Dalyvauja informacinių technologijų saugumo incidentų tyrimuose, nustato jų priežastis ir teikia prevencines priemones.
7.21. Teikia pasiūlymus dėl informacinių technologijų saugumo priemonių diegimo, atnaujinimo ir tobulinimo.
7.22. Rengia ir pristato Valstybės kontrolės darbuotojams informacinių technologijų ir kibernetinio saugumo grėsmių apžvalgas.
7.23. Moko Valstybės kontrolės darbuotojus atpažinti kibernetines grėsmes ir saugiai naudotis informacinėmis technologijomis.

7.24. Pavedus atstovauja Valstybės kontrolei informacinių technologijų saugumo klausimais. 7.25. Vykdo kitus nenuolatinio pobūdžio su departamento veikla susijusius pavedimus.

_____