

**LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO
ĮSTATYMO ĮGYVENDINIMO“ PROJEKTO
DERINIMO PAŽYMA**

Institucijos pavadinimas, rašto data ir numeris	Pastabos ir pasiūlymai	Argumentai, kodėl neatsižvelgta arba tik iš dalies atsižvelgta į suinteresuotų institucijų ir asmenų pastabas ir pasiūlymus
Lietuvos Respublikos sveikatos apsaugos ministerijos 2018-10-18 raštas Nr. 10-7465	2. Siūloma pateikti Metodikos 2 priedo lentelės 2.4., 2.5. 2.8. ir 2.10. punktuose poveikio ypatingos svarbos paslaugos teikimui (toliau – poveikis) vertinimo kriterijų „esminis poveikis“, „didelis poveikis“ ir „nedidelis poveikis“ išaiškinimus ir pateikti šių poveikio kriterijų kiekybines išraiškas, kad būtų galima atlikti objektyvų poveikio ypatingos svarbos paslaugos teikimui įvertinimą.	Atsižvelgta iš dalies. Šiuo metu nurodytų vertinimo kriterijų reikšmės yra atkleidžiamos Infrastruktūros objektų, užtikrinančių ypatingos svarbos paslaugų teikimą, vertinimo klausimyno pildymo rekomendacijose/instrukcijoje. Atsižvelgiant į tai, kad šių reikšmių išaiškinimas yra labiau rekomendacinio pobūdžio, o Ypatingos svarbos informacinės infrastruktūros nustatymo metodikos projektu siūloma nenustatyti teisinio reguliavimo, griežtai draudžiančio atsižvelgti į Atsakingo valdytojo valdomų ryšių ir informacinių sistemų ypatumus (pavyzdžiui, 6.4 papunktyje suteikiama teisė Atsakingai institucijai Klausimyne papildomai nustatyti ir įvertinti jos veiklos srities sektoriaus specifinius kriterijus, galinčius turėti įtakos jos veiklos srityje veikiančių Atsakingų valdytojų veiklai), todėl siūlytina išlaikyti esamą Ypatingos svarbos informacinės infrastruktūros nustatymo metodikos modelį ir tam tikrų reikšmių išaiškinimus laikyti rekomendacinio pobūdžio.
	4. Siūloma Nacionalinio kibernetinių incidentų valdymo plane (toliau – Planas) nustatyti atsakingo informavimo (angl. Responsible Disclosure) apie kibernetinius incidentus ir saugumo spragas tvarką. Pastaruoju metu valstybės įmonė Registrų centras, Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos pagrindinis tvarkytojas, susiduria su neatsakingu informavimu apie kibernetinius incidentus ir saugumo spragas. Praktikoje gali būti sukurtas precedentas, kad informacija apie valstybės informacinių sistemų spragas pirmiau pasieks ne informacinių sistemų valdytojus, o asmenis ir valstybes, keliančias grėsmę	Neatsižvelgta. Siūlymas yra vertas dėmesio, tačiau siūlomi sureguliuoti santykiai yra platesnio pobūdžio nei gali būti reglamentuojama Nacionaliniame kibernetinių incidentų valdymo plane. Siekiant nustatyti atsakingo informavimo apie kibernetinius incidentus ir saugumo spragas tvarką, būtina nustatyti teisę tokią informaciją apskritai gauti teisėtais būdais. Šiuo metu vien savarankiškas informacijos apie kibernetinius incidentus ar saugumo spragas ne savo valdomose ar tvarkomose ryšių ir informacinėse sistemose gavimas yra siejamas su baudžiamosios atsakomybės klausimu, nes Lietuvos Respublikos baudžiamojo kodekso

	<p>Lietuvos nacionaliniam saugumui ir vykdančias priešiškas veiklas pasaulio ir Lietuvos kibernetinėje erdvėje. Remiantis Europos tinklu ir informacijos saugumo agentūros (ENISA), Atviro tinklo programų saugumo projekto (angl. The Open Web Application Security Project (OWASP)) gerąja praktika, apie saugumo spragas pirmiausiai turėtų būti informuojamas sistemos valdytojas, o visuomenės informacijos rengėjų ir skleidėjų atstovai galėtų būti informuojami tada, kai sistemos valdytojas pašalina saugumo spragas, siekiant išvengti asmens duomenų atskleidimo tretiesiems asmenims.</p>	<p>198¹ straipsnis nustato baudžiamąją atsakomybę už neteisėtą prisijungimą prie informacinės sistemos. Sąlygų nustatymas, kurioms esant nebūtų taikoma baudžiamoji atsakomybė, yra įstatymo, o ne įstatymą įgyvendinamųjų teisės aktų, reguliavimo dalykas. Atsižvelgiant į tai, kol kas nėra teisinio pagrindo Lietuvos Respublikos kibernetinio saugumo įstatymą įgyvendinamuosiuose teisės aktuose nustatyti atsakingo informavimo apie kibernetinius incidentus ir saugumo spragas tvarką.</p> <p>Pažymėtina, kad įgyvendinant Nacionalinę kibernetinio saugumo strategiją yra planuojama kurti atsakingą viešojo ir privataus sektorių informacinių ir ryšių technologijų (toliau – IRT) saugumo spragų atskleidimo praktiką. Šis uždavinys bus įgyvendinamas nustatant šios srities veiklos principus, metodų, techninių gebėjimų ar kitų priemonių taikymo tvarką. Kartu pastebėtina, kad Lietuvos Respublikos kibernetinio saugumo įstatyme ir Nacionaliniame kibernetinių incidentų valdymo plane yra nustatoma savanoriško informavimo apie kibernetinius incidentus tvarka, kuri iš dalies sprendžia aprašytą problemą.</p>
	<p>Lietuvos Respublikos sveikatos apsaugos ministerija Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše (toliau – Aprašas) siūlo įvertinti tai, kad:</p> <p>1. reikalavimus rizikos vertinimui jau nustato Bendrieji elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, IV skyrius „Rizikos įvertinimas“.</p> <p>2. Apraše nustatyti techniniai kibernetinio saugumo reikalavimai savo pobūdžiu yra panašūs arba dubliuoja Techniniuose valstybės registrų (kadastrų), žinybinių registrų,</p>	<p>Neatsižvelgta. Nurodyti teisės aktai yra priimti vadovaujantis skirtingais pagrindais. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas yra priimamas Kibernetinio saugumo įstatymo pagrindu, o Bendrųjų elektroninės informacijos saugos reikalavimų aprašas – Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo pagrindu. Valstybės informacinių išteklių valdytojai ir tvarkytojai, kuriems yra taikomas Valstybės informacinių išteklių valdymo įstatymo, o tuo pagrindu ir Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, kartu yra ir kibernetinio saugumo subjektai. Nurodytus įstatymus įgyvendinantys teisės aktai turėtų būti konsoliduojami kompleksiskai, įvertinant ir pačių įstatymų pakeitimo galimybę, pavyzdžiui, Valstybės informacinių išteklių valdymo įstatyme apsiriboti tik nuoroda į Kibernetinio</p>

	<p>valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus ministro 2013 m. spalio 4 d. įsakymu Nr. 1 V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, nustatytus saugos reikalavimus. (pagal Lietuvos Respublikos Vyriausybės 2018 m. sausio 3 d. nutarimo Nr. 20 „Dėl Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimo Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ pakeitimo“ 1.1 papunktį nuo 2018 m. sausio 10 d. techninius informacinių sistemų elektroninės informacijos saugos reikalavimus nustato krašto apsaugos ministras).</p> <p>3. Valstybės kontrolės 2015 m. gruodžio 9 d. valstybinio audito ataskaitoje „Kibernetinio saugumo aplinka Lietuvoje“ Nr. VA-P-90-4-16 buvo pasiūlyta nustatyti bendras kibernetinio saugumo, el. informacijos saugos strategines kryptis ir joms pasiekti būtinas priemones, konsoliduoti elektroninės informacijos saugos valdymą, taip pat skirti įstaigą, kuri koordinuotų šios srities reikalavimų rengimą, jų suvienijimą ir nustatyti lėšų skyrimo, panaudojimo prioritetus ir kriterijus. Krašto apsaugos ir Vidaus reikalų ministerijoms buvo rekomenduota peržiūrėti esamus kibernetinio saugumo, elektroninės informacijos saugos reikalavimus, juos suderinti, patvirtinti šios srities trūkstamas nuostatas, metodinius dokumentus ir numatyti priemones, skirtas konsultuoti ir informuoti kibernetinį saugumą, elektroninės informacijos saugą užtikrinančius subjektus aktualiais šios srities klausimais.</p> <p>Lietuvos Respublikos sveikatos apsaugos ministerija atkreipia Jūsų dėmesį į tai, kad šiuo LRV nutarimo projektu kibernetinio saugumo ir elektroninės informacijos saugos</p>	<p>saugumo įstatymą, taip išvengiant dviejų panašaus pobūdžio teisės aktų rengimo. Atsižvelgiant į tai, kas išdėstyta ir papildomai akcentuojant Kibernetinio saugumo įstatymą įgyvendinantys teisės aktai kartu ir 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL 2016 L 194, p. 1) (toliau – TIS direktyva) nuostatas, į Kibernetinio saugumo įstatymą įgyvendinančius teisės aktus siūlytina neįtraukti elektroninės informacijos saugos ir kibernetinio saugumo sričių reglamentavimo konsolidavimą užtikrinančias teisės normas.</p>
--	--	--

	<p>reglamentavimas nėra keičiamas, todėl išlieka nenuoseklus ir nesistemiškas, o tai praktikoje apsunkina vienas kitą dubliuojančių reikalavimų įgyvendinimą. Kibernetinio saugumo dokumentų turinį reglamentuoja LRV nutarimo projektas, o elektroninės informacinės saugos dokumentų – Saugos dokumentų turinio gairių aprašas, tačiau nurodytų teisės aktų reikalavimai minėtų dokumentų turiniui yra labai panašūs arba dubliuojasi. Siekiant užtikrinti elektroninės informacijos saugos ir kibernetinio saugumo teisinio reguliavimo sistemiškumą ir efektyvumą, siūlome įvertinti galimybę kartu konsoliduoti elektroninės informacijos saugos ir kibernetinio saugumo sričių reglamentavimą, pvz., nustatyti bendrus organizacinius ir techninius elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus, bendrus reikalavimus saugos dokumentų turiniui ir pan.</p>	
<p>Lietuvos Respublikos energetikos ministerijos 2018-10-26 Nr. (10.2-12 E)-3-1943</p>	<p>I. Plano priedas „Kibernetinių incidentų kategorijų sąrašas“ (toliau – Sąrašas), kurį sudaro 4 puslapiai, yra per ilgas ir per sudėtingas, kad būtų galima greitai, tiksliai ir vienareikšmiškai identifikuoti kibernetinio incidento grupę ir kategoriją. Tai išryškėjo pratybų „Kibernetinis skydas 2018“ metu, kai reikėjo praktiškai tai išbandyti. Be to, neaiškios sąraše naudojamos sąvokos ir yra netikslumų.</p> <p>Pateikiame kelis konkrečius pavyzdžius, kurių yra ir daugiau:</p> <ol style="list-style-type: none"> 1. LITGRID AB, kaip kibernetinio saugumo subjektui, buvo sudėtinga identifikuoti skirtumus tarp šių dviejų grupių: <ol style="list-style-type: none"> a) „Aptikta moderni kenkimo programinė įranga (angl. advanced persistent threat, APT),“ b) „Kenkimo programinė įranga, kurios neaptinka įprastos saugumo priemonės“ ir t.t. 2. Pagal Sąrašą tas pats incidentas gali atitikti keletą grupių ir neaišku, kaip tokiu atveju elgtis. 3. LITGRID AB požiūriu, ypač reikšmingai incidentų grupei „RIS aktyviai kontroliuojama įsibrovėlių (pavyzdžiui, „galinės durys (angl. back door), kompiuterizuotos darbo vietos 	<p>Atsižvelgta iš dalies. Patikslintas Planas nurodant, kad Nacionalinio kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – NKSC) gali būti pranešama ir apie kelias kibernetinio incidento grupes. Patikslinta Plano projekto priedo lentelė. Kibernetinio incidentų grupės išskirstytos į pogrupius. Panaikintas pogrupis „Kenkimo programinė įranga, kurios neaptinka įprastos saugumo priemonės“. Atkreiptinas dėmesys, Plano projekto priede įvardinti incidentų grupių aprašymai sudaryti atsižvelgiant į Europos Sąjungos tinklų ir informacijos apsaugos agentūros (angl. European Network and Information Security Agency ENISA) ekspertų sudarytas metodines rekomendacijas ir patarimus dėl incidentų grupių klasifikacijos nustatymo, o kibernetinio incidento poveikio mastas buvo nustatytas atsižvelgiant į TIS direktyvos nuostatas reglamentuojančias incidento poveikio parametrus.</p>

	<p>ar tarnybinės stotys tampa „Botinklo“ (angl. Botnet) infrastruktūros dalimi“, siekiant suteikti kurią nors kategoriją, reikia, kad incidentas atitiktų mažiausiai du poveikio kriterijus. Jei neatitinka dviejų kriterijų, tai netraktuojama net kaip nereikšmingas incidentas. Tuo tarpu „Vykdoma perimetro priemonių žvalgyba, nebandant įsilaužti“ gali įgauti ir vidutinės reikšmės incidento kategoriją (nors nėra aišku kaip tą padaryti, nes žvalgyba poveikio veiklai nedaro, o jei daro, tai jau vadinasi DDoS ir patenka į kitą kategoriją).</p> <p>Atsižvelgiant į tai, siūlome ženkliai koreguoti Sąrašą arba pasilikti prie ankstesnės jo redakcijos.</p>	
<p>Lietuvos Respublikos susisiekimo ministerijos 2018-10-25 raštas Nr. 2-13952</p>	<p>Apibendrinant tai, kas išdėstyta, Susisiekimo ministerijai kyla klausimas, ar šiuo teikiamu derinti Nutarimo projektu pateiktas Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo projektas (toliau – aprašo projektas) laikytinas Nacionalinam saugumui užtikrinti svarbių objektų apsaugos įstatymo 18 straipsnio 1 dalyje numatytais kibernetinio saugumo reikalavimais. Jei tai tie patys reikalavimai, siūlytume nutarimo preambulėje ar aprašo projekto bendrosiose nuostatose šią sąsają paminėti, kadangi susidaro neapibrėžta situacija, kai įmonės, kurioms reikia parengti saugos planus, negali įvertinti kokius ir kokia apimtimi taikyti kibernetinės saugos reikalavimus parenkant priemones Nacionalinam saugumui užtikrinti svarbių objektų apsaugos įstatymo kontekste. Taip pat nėra aišku, nuo kurios datos turi būti pradėtas skaičiuoti minėtas 2 mėnesių terminas, per kurį įmonės turi parengti saugos planų projektus.</p>	<p>Neatsižvelgta. Nacionalinam saugumui užtikrinti svarbių objektų apsaugos įstatymo 18 straipsnio 1 dalyje kalbama apie galimybę patvirtinti kibernetinio saugumo reikalavimus, kiek jų nereglamentuoja Lietuvos Respublikos kibernetinio saugumo įstatymas. Atsižvelgiant į tai, kad Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo projektu yra tiesiogiai įgyvendinamas Kibernetinio saugumo įstatymo 5 straipsnio 4 punktas, kas reiškia, kad šiuo projektu reglamentuojami santykiai yra Kibernetinio saugumo įstatymo reguliavimo dalykas, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo projektas reguliuojami santykiai negali būti laikomi kibernetinio saugumo reikalavimais, nurodytais Nacionalinam saugumui užtikrinti svarbių objektų apsaugos įstatymo 18 straipsnio 1 dalyje.</p>
<p>Lietuvos banko 2018-10-26 raštas Nr. S 2018/(26.4-2600)-12-5560</p>	<p>1.2. Manome, kad Aprašo III skyriuje pateikti reikalavimai yra per griežti:</p> <p>a) 6.1 punkte rizikos vertinimą siūlome atlikti kartą per 2 metus, arba kaskart po to, kai įvyksta esminių organizacinių ar sisteminių pokyčių;</p>	<p>Neatsižvelgta. Bendrojo elektroninės informacijos saugos reikalavimų aprašo 35 punktas nustato kasmetinį valstybės informacinių sistemų rizikos įvertinimą. Siekiant suvienodinti reikalavimus subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinių išteklius, įpareigojimas atlikti rizikos vertinimą Apraše taip pat yra nustatomas kasmetinis. Atsižvelgiant į tai, kad ypatingos svarbos informacinės infrastruktūra apskritai yra laikoma pačia</p>

		svarbiausia infrastruktūra, jos valdytojams reikalavimai šiuo aspektu nustatomi kaip ir subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinių išteklius.
	b) 6.3 punkte teigiama, kad visi kibernetinio saugumo dokumentai turi būti suderinti su NKSC. Informuojame, kad Lietuvos banke yra atskiri dokumentai ir taisyklės kiekvienai sričiai, tad kiekvieno iš jų derinimas su NKSC yra perteklinis reikalavimas. Siūlome sumažinti teikiamų dokumentų apimtį ir patikslinti, kurie dokumentai, skirti bendrai (ne tik YSII) organizacijos veiklai, turi būti tik pateikiami NKSC. Derinami turėtų būti tik tie dokumentai, kurie tiesiogiai reglamentuoja YSII veikimą.	Neatsižvelgta. Vadovaujantis Aprašo 6.3 papunkčiu, su NKSC reikia derinti tik tuos teisės aktus, kurie reglamentuoja valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros kibernetinio saugumo politiką ir jos įgyvendinimą, kartu nustatant, kad nurodytuose teisės aktuose turi būti įtvirtinta. Teisės aktų, nesusijusių su 6.3 papunktyje nurodytu reguliavimo dalyku derinti su NKSC nereikia, todėl kiekvienas subjektas, taikantis Aprašą, turėtų pats pasirinkti vidinių teisės aktų tvirtinimo politiką taip, kad jų derinimas su valstybės institucijomis netaptų perteklinis.
	c) 9 punkte siūlome, kad kibernetinio saugumo dokumentai turi būti peržiūrimi (persvarstomi) ne rečiau kaip kartą per 2 metus.	Neatsižvelgta. Kibernetinio saugumo dokumentų peržiūrėjimas yra derinimas su rizikos vertinimu. Atsižvelgiant į tai, kad rizikos vertinimui yra nustatomas 1 metų ciklas, tokio paties ciklo turi būti laikomasi ir peržiūrint kibernetinio saugumo dokumentus. Pastebėtina, kad reikalavimas yra <i>peržiūrėti</i> kibernetinio saugumo dokumentus, tačiau peržiūrėjimas nebūtinai reiškia keitimą.
Lietuvos Respublikos vidaus reikalų ministerijos 2018-11-02 raštas Nr. 1D-5399	1. Mūsų vertinimu nutarimo projekte tvirtinamas Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas (toliau – Aprašas) iš dalies dubliuoja Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu 716, reglamentavimo objektą (pvz., rizikos vertinimas, atitikties vertinimas, saugos įgaliotinio funkcijos), todėl sukuriamas papildomas teisinis neapibrėžtumas, teisės normų kolizijos ir konkurencijos atvejai. Mūsų nuomone turėtų būti oš esmės sprendžiamas klausimas kibernetinio saugumo ir elektroninės informacijos saugos reglamentavimo konsolidavimo. Iki to siūlome Apraše teikti aiškias, teisiškai korektiškas nuorodas į Bendrųjų elektroninės informacijos saugos reikalavimų aprašo nuostatas, kurios papildomos kibernetinio saugumo reikalavimais.	Atsižvelgta iš dalies. Nurodyti teisės aktai yra priimami vadovaujantis skirtingais pagrindais. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas yra priimamas Kibernetinio saugumo įstatymo pagrindu, o Bendrųjų elektroninės informacijos saugos reikalavimų aprašas – Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo pagrindu. Valstybės informacinių išteklių valdytojai ir tvarkytojai, kuriems yra taikomas Valstybės informacinių išteklių valdymo įstatymo, o tuo pagrindu ir Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, kartu yra ir kibernetinio saugumo subjektai. Nurodytus įstatymus įgyvendinantys teisės aktai turėtų būti konsoliduojami kompleksiskai, įvertinant ir pačių įstatymų pakeitimo galimybę, pavyzdžiui, Valstybės informacinių išteklių valdymo įstatyme apsiriboti tik nuoroda į Kibernetinio

		<p>saugumo įstatymą, taip išvengiant dviejų panašaus pobūdžio teisės aktų rengimo. Atsižvelgiant į tai, kas išdėstyta, į Kibernetinio saugumo įstatymą įgyvendinančius teisės aktus siūlytina neįtraukti elektroninės informacijos saugos ir kibernetinio saugumo sričių reglamentavimo konsolidavimą užtikrinančių teisės normų.</p> <p>Kartu pabrėžtina, kad Aprašas yra taikomas visiems kibernetinio saugumo subjektams, o ne vienai grupei, be to, Apraše nustatomi reikalavimai yra parengti atsižvelgiant į TIS direktyvos nuostatas, todėl nuorodos į Bendrųjų elektroninės informacijos saugos reikalavimų aprašo nuostatas yra teikiamos tik subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ir ypatingos svarbos informacinės infrastruktūros valdytojams.</p>
	<p>6. Nesuprantamas nutarimo projekte tvirtinamo Nacionalinio kibernetinių incidentų valdymo plano (toliau – Planas) 1.5 ir 25.12 papunkčiuose nustatytų reikalavimų pateikti tikslų laiką (ateityje), kada bus teikiama Plano reikalaujama informacija, poreikis ir prasmė. Manome, kad Plane reglamentuoti informacijos pateikimo terminai yra pakankamas reikalavimas kibernetinio incidentų valdymo procesui, todėl siūlome minėtų perteklinių reikalavimų atsisakyti.</p>	<p>Neatsižvelgta. Reikalavimas nurodyti tikslų laiką yra nustatomas siekiant gerinti komunikaciją tarp kibernetinio saugumo subjektų ir NKSC. Plane yra nustatomas pakankamai ilgas kibernetinio incidento tyrimo ataskaitos pateikimo terminas (didelio poveikio kibernetinių incidentų atveju 4 valandos, vidutinio poveikio – 24 valandos), kuris ne visais atvejais būtinas valdant kibernetinį incidentą. Siekiama skatinti kibernetinio saugumo subjektus įsivertinti kibernetinio incidento valdymo galimybes ir pačiam nusistatyti terminus, kada bus teikiama reikalaujama informacija. Tokiu būdu, visų pirma, būtų užtikrinama, kad į kibernetinio saugumo subjekto pateiktą informacijos bus reaguojama jau informacijos gavimo momentu ir tokiu būdu taupomas laikas, be to, būtų sudaromos sąlygos NKSC vertinti, kaip yra valdomas kibernetinis incidentas, t. y. pagal tai, ar kibernetinio saugumo subjektui pavyksta laikytis savo paties nusistatyto termino, galima spręsti ir apie kibernetinio incidento valdymo sėkmę.</p>

Utenos Respublikos
vidaus reikalų departamentas
Eilutės numeras

2018-11-06

Krašto apsaugos komisijos

Edvinas Kerz