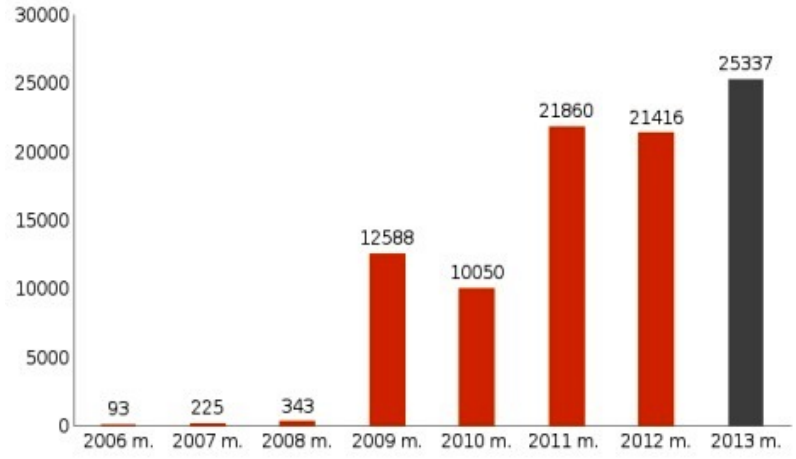
NUMATOMO TEISINIO REGULIAVIMO PRIORITETINIŲ TEISĖKŪROS INICIATYVŲ POVEIKIO VERTINIMO PAŽYMA

Prioritetinės teisėkūros iniciatyvos pavadinimas	Kibernetinio saugumo srities reglamentavimas
Vertinimą atlikusi institucija	Lietuvos Respublikos vidaus reikalų ministerija
Problema	Nuolat tobulėjant informacijos ir ryšių technologijoms ir didėjant jų naudojimui visuomeniniame gyvenime, atitinkamai sparčiai didėja šių technologijų panaudojimas siekiant kam nors (asmenims, valstybei) pakenkti. Nuolat didėjant kibernetinių incidentų, kibernetinių atakų skaičiui ir mastui, būtina sukurti tiek teisinę, tiek fizinę aplinką, kuri būtų saugi, atspari, greitai reaguojanti į kibernetinius incidentus ir taip padedanti išvengti galimos žalos. Šiuo metu Lietuvoje kibernetinis saugumas dažniausiai užtikrinamas individualiai, dalis privataus sektoriaus atstovų rūpinasi savo saugumu, dalis jų – nesirūpina išvis. Valstybės institucijos taip pat dažniausiai rūpinasi tik savo valdomų informacinių išteklių saugumu. Vieni juridiniai asmenys turi geresnę techninę įrangą, žinias ir patirtį šioje srityje ir gali tinkamai pasirūpinti savo išteklių kibernetiniu saugumu, kiti – nepakankamai arba išvis negali, taip keldami grėsmę patirti žalą ne tik sau, bet ir kitiems juridiniams ir fiziniams asmenims ar net visai valstybei, pavyzdžiui, mažoje, nesvarbioje informacinėje sistemoje prasidėjęs kibernetinis incidentas nevaldomai gali išaugti ir pradėti kenkti kitoms informacinėms sistemoms, pramonės valdymo informacinėms sistemoms ar elektroninių ryšių tinklams ir taip daryti žalą kitiems asmenims ar sukelti pavojų žmonių sveikatai, valstybės saugumui ar jos funkcijų vykdymui. Taip pat Lietuvoje nėra nustatytos kibernetinių grėsmių valdymo sistemos, nėra institucijų, atsakingų už kibernetinių incidentų valdymą, jo koordinavimą. Tą įrodo Lietuvoje įvykusios kibernetinės atakos, viešai aprašytos žiniasklaidos, kai atakuojamų informacinių sistemų ir techninės įrangos savininkai patys negalėjo apsisaugoti nuo didėjančios kibernetinės atakos, nežinojo į ką kreiptis ir ką turėtų daryti, kad kibernetinis incidentas būtų suvaldytas. Didėjantį kibernetinių incidentų kiekį galima pastebėti pagal Lietuvos Respublikos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio (toliau – CERT-LT) ištirtų incidentų ataskaitą:

	 Tikrasis kibernetinių incidentų kiekis yra daug didesnis, kadangi daug juridinių asmenų, nerizikuodami savo reputacija, neinformuoja kompetentingų institucijų apie įvykusius incidentus. Taip pat pagal CERT-LT ataskaitą nuolat didėja ir kibernetinių incidentų mastas, pavyzdžiui, 2013 m. buvo fiksuotos iki 6Gb/s elektroninės paslaugos trikdymo atakos prieš taikinius Lietuvoje.
Tikslas	Kibernetinio saugumo srities reglamentavimo tikslas yra nustatyti kibernetinių incidentų valdymo tvarką, valstybės institucijų kompetencijas kibernetinio saugumo srityje, viešojo, privataus sektorių ir akademinės bendruomenės bendradarbiavimą, siekiant užtikrinti ir gerinti kibernetinio saugumo situaciją Lietuvoje. Nustatyti minimalius organizacinius ir techninius reikalavimus informacinių sistemų, pramonės valdymo sistemų ir elektroninių ryšių tinklams, kuriuos atitinkant būtų pagerinta šių infrastruktūrų kibernetinio saugumo situacija, taip pat sumažėtų galimybė patirti didelę žalą įvykus kibernetinio saugumo incidentui. Be to, tikslas yra nustatyti šios infrastruktūros valdytojams – valstybės informacinių išteklių valdytojams, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams ir elektroninės informacijos prieglobos paslaugų teikėjams pareigas ir atsakomybes.
	Status quo Nesiėmus jokių veiksmų, kibernetinio saugumo sritis išliktų reglamentuota fragmentiškai ir nenuosekliai, nebūtų veikiančios nacionalinės kibernetinių incidentų valdymo sistemos, išliktų grėsmė valstybei patirti didelę žalą, vykdyti savo funkcijas ar net netekti suvereniteto dėl įvykusių, nevaldomų kibernetinių incidentų. ***1-oji alternatyva***: Įgyvendinant 1-ąją alternatyvą Lietuvos Respublikos kibernetinio saugumo įstatymu būtų sukurtas centralizuotas kibernetinio saugumo reglamentavimo modelis – kibernetinio saugumo politiką formuotų ir įgyvendintų po vieną valstybės instituciją. ***2-oji alternatyva:*** Įgyvendinant 2-ąją alternatyvą Lietuvos Respublikos kibernetinio saugumo įstatymu būtų sukurtas decentralizuotas kibernetinio saugumo reglamentavimo

	modelis – būtų paskirta pagrindinė institucija, formuojanti kibernetinio saugumo politiką ir kelios kitos institucijos, dalyvaujančios politikos formavime, o politiką pagal kompetenciją įgyvendintų kelios institucijos.
Poveikis kibernetinio saugumo sričiai	***Status quo*** Nieko neatliekant, ateityje kibernetinio saugumo situacija Lietuvoje tik prastėtų, nuolat didėtų rizika valstybei patirti didelę finansinę žalą, sutrikdyti žmonių sveikatą ar prarasti suverenitetą, įvykus kibernetiniams incidentams. Valstybės informacinių išteklių valdytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, elektroninės informacijos prieglobos paslaugų teikėjai ir viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai individualiai rūpinasi savo valdomų infrastruktūrų saugumu, tačiau, esant dideliam kibernetiniam incidentui, individualiai apsisaugoti būtų praktiškai neįmanoma, o kibernetiniam incidentui išplitus po kitas infrastruktūras poveikis valstybei gali būti milžiniškas – valstybės gyventojai likti be šildymo, elektros energijos ar sutrikdytos transporto, bankinės sistemos, valstybės paslaugų teikimas ir pan. Dėl to šalyje gali kilti gyventojų nepasitikėjimas valdžia, viešosios tvarkos pažeidimai ar kitaip destabilizuota situacija. Kiek tiksliai reikėtų valstybės biudžeto lėšų apskaičiuoti neįmanoma, nes lėšų kiekis priklauso nuo daug veiksnių: informacinės infrastruktūros, kurioje įvyktų kibernetinis incidentas, naudojimo paskirties, kibernetinio incidento masto ir trukmės, jei būtų pasisavinami duomenys, neįmanoma įvertinti, ar jie nebus panaudoti kitą kartą ir pan. Kibernetinis saugumas Lietuvoje būtų užtikrinamas nenuosekliai ir aplaidžiai. ***1-oji alternatyva*** Įgyvendinant 1-ąją alternatyvą būtų iš esmės sukurtos kibernetinio saugumo užtikrinimo ir kibernetinių incidentų valdymo sistemos: paskirtos konkrečios institucijos, atsakingos už kibernetinio saugumo politikos formavimą, koordinavimą, kontroliavimą (Lietuvos Respublikos krašto apsaugos ministerija) ir įgyvendinimą (Nacionalinis kibernetinio saugumo centras), nustatytos jų funkcijos ir kompetencijos. Vykdant institucijų organizacinę pertvarką, viską koncentruojant vienoje institucijoje, tikėtina, kad kibernetinio saugumo užtikrinimą tektų pradėti kurti iš naujo, nes esamas įdirbis ir bendradarbiavimo sąryšiai būtų praktiškai sunaikinti. Taip pat įgyvendinant alternatyvą būtų nustatytos valstybės informacinių išteklių valdytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, elektroninės informacijos prieglobos paslaugų teikėjų ir viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų teisės ir pareigos kibernetinio saugumo srityje, minimalieji organizaciniai ir techniniai reikalavimai jų valdomai infrastruktūrai bei atsakomybės už nustatytų pareigų nevykdymą. Kadangi būtų sukurtas centralizuotas modelis, tai už kibernetinio saugumo politikos įgyvendinimą atsakinga valstybės institucija koordinuotų, kontroliuotų ir bendradarbiautų su valstybės informacinių išteklių valdytojais, ypatingos svarbos informacinės infrastruktūros valdytojais, elektroninės informacijos prieglobos paslaugų teikėjais ir viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjais dėl kibernetinių incidentų valdymo, prevencijos ir bendros kibernetinio saugumo situacijos Lietuvoje gerinimo. Įgyvendinus šią alternatyvą, būtų sukurti pamatai kibernetinio saugumo situacijai

	Lietuvoje gerinti ir stiprinti, ženkliai sumažėtų galimybė valstybei patirti didelę žalą, būtų sukurta saugi kibernetinė erdvė, kurioje Lietuvos gyventojai jaustųsi saugiau, mažiau bijotų naudojantis elektroninėmis paslaugomis prarasti duomenis (tarp kurių ir asmens duomenys), padidėtų pasitikėjimas valdžia, jos darbais nacionalinio saugumo situacijos gerinimui. Įgyvendinant alternatyvą, tiesiogiai bus paveikiami viešojo administravimo subjektai, valdantys valstybės informacinius išteklius ir kiti juridiniai asmenys, valdantys ypatingos svarbos informacinę infrastruktūrą, ir (arba) teikiantys viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugas ar elektroninės informacijos prieglobos paslaugas. Šiems subjektams bus nustatyti minimalūs organizaciniai ir techniniai kibernetinio saugumo reikalavimai, kuriais vadovaujantis jų valdomoje infrastruktūroje pagerės kibernetinio saugumo situacija. Atsižvelgiant į šios infrastruktūros svarbą ir galimą poveikį, bus nustatomi diferencijuoti reikalavimai, t. y. kuo informacinė infrastruktūra svarbesnė ir jos galima sukelti žala yra didesnė, tuo jai bus nustatomi didesni reikalavimai. Numatoma, kad nustatomi kibernetinio saugumo reikalavimai neturėtų pareikalauti papildomų jų valdytojų investicijų. Taip pat įgyvendinama alternatyva netiesiogiai paveiks asmenis, kurie naudojasi paslaugomis, kurioms suteikti naudojami valstybės informaciniai ištekliai ar ypatingos svarbos informaciniai ištekliai, arba viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugomis, arba elektroninės informacijos prieglobos paslaugomis. Asmenys patirs naudą, kadangi bus užtikrintas gaunamų paslaugų prieinamumas ir šių paslaugų kibernetinis saugumas. Kadangi kibernetinis saugumas yra labai svarbus aspektas ir ypatingai aktualus šiais informacinės visuomenės laikais, alternatyva turėtų būti įgyvendinama labai skubiai. ***2-oji alternatyva*** Įgyvendinant 2-ąją alternatyvą būtų iš esmės sukurtos kibernetinio saugumo užtikrinimo ir kibernetinių incidentų valdymo sistemos, paremtos bendradarbiavimo principu, t. y.: būtų nustatyta pagrindinė institucija, formuojanti kibernetinio saugumo politiką (Krašto apsaugos ministerija), bei kitos valstybės institucijos, pagal kompetenciją dalyvaujančios politikos formavime (Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija, Vidaus reikalų ministerija, Policijos departamentas prie Vidaus reikalų ministerijos). Taip pat nustatytos institucijos, pagal kompetenciją įgyvendinančios kibernetinio saugumo politiką (Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija, Policijos departamentas prie Vidaus reikalų ministerijos). Kibernetinio saugumo užtikrinimas ir kibernetinių incidentų valdymas būtų paremtas tarpinstituciniu bendradarbiavimu pagal patvirtintą nacionalinį incidentų valdymo planą. Išlaikant kompetencijas atskirose institucijoje, nebūtų griaunama esama institucijų funkcinė sąranka, o naujos funkcijos, kurios šiuo metu nėra atliekamos, būtų priskirtos esamoms institucijoms arba perduotos institucijai (Nacionaliniam kibernetinio saugumo centrui), iš esmės atsakingai už kibernetinio saugumo politikos įgyvendinimą. Įgyvendinant šią alternatyvą būtų nustatytos valstybės informacinių išteklių valdytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, elektroninės

	informacijos prieglobos paslaugų teikėjų ir viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų teisės ir pareigos kibernetinio saugumo srityje, minimalieji organizaciniai ir techniniai reikalavimai jų valdomai infrastruktūrai bei atsakomybės už nustatytų pareigų nevykdymą. Kadangi būtų sukurtas decentralizuotas modelis, tai už kibernetinio saugumo politikos įgyvendinimą atsakingos valstybės institucijos pagal kompetenciją kontroliuotų, kaip šių reikalavimų yra laikomasi: Nacionalinis kibernetinio saugumo centras – kontroliuotų valstybės informacinių išteklių valdytojus ir ypatingos svarbos informacinės infrastruktūros valdytojus. Ryšių reguliavimo tarnyba – reguliuotų elektroninės informacijos prieglobos paslaugų teikėjus ir viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjus. Taip pat būtų sukurta Kibernetinio saugumo taryba, sudaryta iš viešojo, privataus sektoriaus ir akademinės bendruomenės atstovų, kurios tikslas bendradarbiaujant visiems sektoriams stiprinti kibernetinio saugumo situaciją Lietuvoje. Įgyvendinant šią alternatyvą, būtų stiprinama esama kibernetinio saugumo situacija Lietuvoje, padengiamos kibernetinio saugumo „pilkos dėmės“, todėl sumažėtų galimybė valstybei patirti didelę žalą, būtų sukurta saugi kibernetinė erdvė, kurioje Lietuvos gyventojai jaustųsi saugiau, taip pat padidėtų pasitikėjimas valdžia, jos darbais nacionalinio saugumo situacijos gerinimui. Įgyvendinant alternatyvą, tiesiogiai bus paveikiami viešojo administravimo subjektai, valdantys valstybės informacinius išteklius, ir kiti juridiniai asmenys, valdantys ypatingos svarbos informacinę infrastruktūrą, ir (arba) teikiantys viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugas ar elektroninės informacijos prieglobos paslaugas. Šiems subjektams bus nustatyti minimalūs organizaciniai ir techniniai kibernetinio saugumo reikalavimai, kuriais vadovaujantis jų valdomoje infrastruktūroje pagerės kibernetinio saugumo situacija. Atsižvelgiant į šios infrastruktūros svarbą ir galimą poveikį, bus nustatomi diferencijuoti reikalavimai, t. y. kuo informacinė infrastruktūra svarbesnė ir jos galima sukelti žala yra didesnė, tuo jai bus nustatomi didesni reikalavimai. Numatoma, kad nustatomi kibernetinio saugumo reikalavimai neturėtų pareikalauti papildomų jų valdytojų investicijų. Taip pat įgyvendinama alternatyva netiesiogiai paveiks ir asmenis, kurie naudojasi paslaugomis, kurioms suteikti naudojami valstybės informaciniai ištekliai ar ypatingos svarbos informaciniai ištekliai, arba viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugomis, arba elektroninės informacijos prieglobos paslaugomis. Asmenys patirs naudą, kadangi bus užtikrintas gaunamų paslaugų prieinamumas ir šių paslaugų kibernetinis saugumas. Kadangi kibernetinis saugumas yra labai svarbus aspektas ir ypatingai aktualus šiais informacinės visuomenės laikais, alternatyva turėtų būti įgyvendinama labai skubiai.
Poveikis valstybės finansams	***Status quo*** Vidaus reikalų ministerija atliko valstybės ir savivaldybių institucijų apklausą dėl kibernetinio saugumo užtikrinimo priemonių vykdymo. Pagal gautus rezultatus pastebėta, kad dauguma vykdomos tos kibernetinio saugumo užtikrinimo priemonės, kurios nereikalauja papildomų lėšų. Iš 110 institucijų net 32 institucijos nurodė, kad specialiai kibernetiniam saugumui užtikrinti lėšų neskiriama. Pagal

pateiktus duomenis vidutiniškai institucija kibernetiniam saugumui užtikrinti skiria 115 tūkst. Lt.

Nereglamentavus kibernetinio saugumo srities papildomų valstybės ir savivaldybių biudžeto lėšų kibernetiniam saugumo užtikrinimui nereikėtų, tačiau, įvykus didelio masto kibernetiniams incidentams, kurie sutrikdytų valstybės funkcijų vykdymą ar pakenktų ūkio (pavyzdžiui, energetikai ar bankininkystei) šakai, gali būti patirta labai didelė žala, kuri, priklausomai nuo kibernetinio incidento dydžio ir objekto, gali būti įvertinta nuo kelių milijonų iki kelių šimtų milijonų litų. Preliminariai įvertinti galimą žalą valstybei yra neįmanoma, kadangi daug faktorių, lemiančių žalos dydį, priklauso nuo objekto, prieš kurį nukreiptas kibernetinis incidentas, kibernetinio incidento dydžio, jo trukmės ir tipo. Kaip kibernetinio incidento padarytos žalos dydžio pavyzdį, galima įvertinti naujienų portalui Delfi.lt padarytą žalą po kibernetinės atakos, tuo metu buvo įvertinta 350 tūkst. Lt žala. Analizuojant žalos dydį reikėtų įvertinti tai, kad kibernetinis incidentas truko apie dvi savaites, kurio metu naujienų portalas dalį laiko nebuvo prieinamas visiems vartotojams, o kitą dalį tik nesantiems Lietuvos teritorijoje.

1-oji alternatyva

Įgyvendinant 1-ąją alternatyvą ir kuriant centralizuotą kibernetinio saugumo užtikrinimo sistemą, naujų funkcijų vykdymui steigiamame Nacionaliniame kibernetinio saugumo centre reikės naujų pareigybių. Naujos pareigybės reikalingos atlikti funkcijas, nurodytas „poveikio vertinimo administracinei naštai“ skiltyje prie 1-osios alternatyvos.

Krašto apsaugos ministerijos srities institucijai arba jos padaliniui – Nacionaliniam kibernetinio saugumo centrui funkcijoms vykdyti iš viso reikėtų 40 pareigybių. Iš kurių 12 naujų pareigybių reikia 2015 m., papildomai 16 – 2016 m., kitos pareigybės būtų perkeltos iš kitų Krašto apsaugos ministerijos srities institucijų ir kitų institucijų, šiuo metu dalyvaujančių kibernetinio saugumo užtikrinimo veikloje.

Atsižvelgiant į tai, papildomas lėšų poreikis darbo užmokesčiui, apskaičiuotam pagal Valstybės tarnautojų ir darbuotojų, gaunančių darbo užmokestį iš Lietuvos Respublikos valstybės biudžeto, savivaldybių biudžetų ir valstybės pinigų fondų, darbo užmokesčio fondo apskaičiavimo metodiką (toliau – metodika), patvirtintą Lietuvos Respublikos Vyriausybės 2003 m. kovo 3 d. nutarimu Nr. 280:

Pareigybė (karjeros VT)	*Pareig. kate-gorija*	*Kvalifikacinė klasė*			*Skaičius*			*Lėšų poreikis*					
		2015 metai	2016 metai	2017 metai	2015 metai	2016 metai	2017 metai	2015 metai		2016 metai		2017 metai	
								DU	Soc. draud. įmokos	DU	Soc. draud. įmokos	DU	Soc. draud. įmokos
Direktoriaus pavaduotojas	*A18*	II	I	I	1	1	1	75,8	23,5	87,5	27,1	87,5	27,1
Skyriaus vedėjas	*A16*	III	II	I	2	2	2	108,1	33,5	122,1	37,9	140,9	43,7
Poskyrio vedėjas	*A14*	III	II	I	2	2	2	86,9	26,9	98,3	30,5	113,4	35,2
Vyr. specialistas	*A13*	III	II	I	7	23	23	273,9	84,9	1017,2	315,3	1173,7	363,8
				Iš viso:				544,7	168,8	1325,1	410,8	1515,5	469,8
				Priemokoms 5 %:						66,3	20,5	75,8	23,5

Iš viso:	**544,7**	**168,8**	**1391,4**	**431,3**	**1591,3**	**493,3**

Papildomas lėšų poreikis kitoms išlaidoms 2015 m. sudarys apie 3650 tūkst. Lt, 2016 m. – apie 750 tūkst. Lt, o 2017 m. ir paskesniais metais – apie 800 tūkst. Lt. Nurodytas kitų išlaidų lėšų poreikis apima lėšų poreikį specialistų kvalifikacijai kelti, mokėjimams už komunalines ir ryšių paslaugas, taip pat įmokas už narystę tarptautinių organizacijų duomenų bazėse, techninės ir programinės įrangos perkėlimo į Nacionalinį kibernetinio saugumo centrą, techninės ir programinės įrangos priežiūros paslaugas ir kitas su veikla susijusias išlaidas.

Papildomas lėšų poreikis turtui įsigyti 2015 m. bus apie 2007,9 tūkst. Lt, 2016 m. – apie 4555,6 tūkst. Lt, o 2017 m. – apie 1104,8 tūkst. Lt. Šios lėšos apimtų investicijų projektus, skirtus patalpoms įrengti, sutvarkyti ir darbo vietoms įkurti, taip pat darbo vietos įrangai, bei kitai įrangai, skirtai kibernetiniam saugumui užtikrinti, įsigyti.

Asignavimų poreikis, tūkst. Lt	**Metai**		
	2015	**2016**	**2017 ir vėliau**
Išlaidoms	4363,5	2572,7	2884,6
– iš jų darbo užmokesčiui	*544,7*	*1391,4*	*1591,3*
– iš jų socialinio draudimo įmokoms iš darbdavio lėšų	*168,8*	*431,3*	*493,3*
Turtui įsigyti	3207,9	4555,6	1604,8
IŠ VISO	**7571,4**	**7128,3**	**4489,4**

2-oji alternatyva

Įgyvendinant 2-ąją alternatyvą ir kuriant decentralizuotą kibernetinio saugumo užtikrinimo sistemą, naujų funkcijų vykdymui Nacionaliniame kibernetinio saugumo centre reikės naujų pareigybių. Naujos pareigybės reikalingos atlikti naujas funkcijas, nurodytas „poveikio vertinimo administracinei naštai“ skiltyje prie 2-osios alternatyvos.

Krašto apsaugos ministerijos srities institucijai arba jos padaliniui – Nacionaliniam kibernetinio saugumo centrui, funkcijoms vykdyti iš viso būtų reikalingos 25 pareigybės. Iš kurių 8 naujos pareigybės reikalingos 2015 m., papildomai 10 – 2016 m., kitos pareigybės būtų perkeltos iš kitų Krašto apsaugos ministerijos srities institucijų.

Pagal metodiką atlikus skaičiavimus, nustatytas papildomas lėšų poreikis darbo užmokesčiui:

Pareigybė (karjeros VT)	***Pareig. kate-***	***Kvalifikacinė klasė***	***Skaičius***	***Lėšų poreikis***

	gorija	2015 metai	2016 metai	2017 metai	2015 metai	2016 metai	2017 metai	2015 metai		2016 metai		2017 metai	
								DU	Soc. draud. įmokos	DU	Soc. draud. įmokos	DU	Soc. draud. įmokos
Direktoriaus pavaduotojas	*A18*	II	I	I	1	1	1	75,8	23,5	87,5	27,1	87,5	27,1
Skyriaus vedėjas	*A16*	III	II	I	1	1	1	54,0	16,7	61,1	19,0	70,5	21,2
Poskyrio vedėjas	*A14*	III	II	I	1	1	1	43,5	13,5	49,1	15,2	56,7	17,6
Vyr. specialistas	*A13*	III	II	I	5	15	15	195,6	60,6	663,4	205,7	765,5	237,3
							Iš viso:	368,9	114,3	861,1	267,0	980,2	303,2
							Priemokoms 5 %:			43,2	13,4	49,0	15,3
							Iš viso:	**368,9**	**114,3**	**904,2**	**280,4**	**1029,2**	**318,4**

Papildomas lėšų poreikis kitoms išlaidoms 2015 m. sudarys apie 560 tūkst. Lt, 2016 m. – apie 620 tūkst. Lt, o 2017 m. ir paskesniais metais – apie 720 tūkst. Lt. Nurodytas kitų išlaidų lėšų poreikis apima lėšų poreikį Nacionalinio kibernetinio saugumo centro darbuotojų kvalifikacijai kelti, mokėjimams už komunalines ir ryšių paslaugas, taip pat įmokas už narystę tarptautinių organizacijų duomenų bazėse ir kitas su veikla susijusias išlaidas.

Papildomas lėšų poreikis turtui įsigyti 2015 m. bus apie 2 067,9 tūkst. Lt, 2016 m. – apie 4 615,6 tūkst. Lt, o 2017 m. – apie 1 104,8 tūkst. Lt. Šios lėšos apimtų investicijų projektus, skirtus steigiamo Nacionalinio kibernetinio saugumo centro patalpoms įrengti, sutvarkyti ir darbo vietoms įkurti (jų įrangai įsigyti), taip pat įrangai, skirtai kibernetiniam saugumui užtikrinti, įsigyti.

Preliminarus papildomų lėšų poreikis Nacionaliniam kibernetinio saugumo centrui steigti ir veiklai vykdyti 2015–2017 m. taip pat pateiktas lentelėje:

Asignavimų poreikis, tūkst. Lt	**Metai**		
	2015	**2016**	**2017 ir vėliau**
Išlaidoms	1043,2	1804,6	2067,6
– iš jų darbo užmokesčiui	*368,9*	*904,2*	*1029,2*
– iš jų socialinio draudimo įmokoms iš darbdavio lėšų	*114,3*	*280,4*	*318,4*
Turtui įsigyti	2067,9	4615,6	1104,8
IŠ VISO	**3111,1**	**6420,2**	**3172,4**

Projekto 1-osios ir 2-osios alternatyvų įgyvendinimas nepaveiks valstybės tarptautinių finansinių įsipareigojimų, o alternatyvų įgyvendinimui reikiamos išlaidos turėtų būti finansuojamos perskirstant valstybės biudžetą.

<table>
<tr><td></td><td>Viešojo administravimo subjektai, valdantys valstybės informacinius išteklius, nustatytus kibernetinio saugumo reikalavimus įgyvendinti naudos turimas institucijos biudžeto lėšas (kaip daroma ir šiuo metu).</td></tr>
<tr><td>Poveikis administracinei naštai</td><td>
Status quo
Šiuo metu valstybės ir savivaldybių institucijos informacinius įpareigojimus vykdo pagal Bendrųjų elektroninės informacijos saugos reikalavimų aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716. Valstybės ir savivaldybių institucijos apie įvykusius elektroninės informacijos saugos incidentus turi informuoti kompetentingas institucijas.
Poveikis piliečių ir kitų asmenų administracinei naštai nenumatomas.

1-oji ir 2 alternatyvos.
Poveikis valstybės ir savivaldybių institucijų ir įstaigų administracinei naštai nepasikeistų.
Pagal Lietuvos Respublikos Vyriausybės 2012 m. sausio 11 d. nutarimu Nr. 4 patvirtintą Administracinės naštos ūkio subjektams nustatymo metodiką buvo vertinama elektroninės informacijos prieglobos paslaugų teikėjų ir viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų administracinė našta vykdant informacinį įpareigojimą.
Parengti ir užpildyti klausimynai 2014 m. gegužės 12 d. buvo išsiųsti 40 elektroninės informacijos prieglobos paslaugų teikėjų ir 40 viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų. Atsakymus pateikė 10 elektroninės informacijos prieglobos paslaugų teikėjų ir 13 viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų. Pagal pateiktus atsakymus paskaičiuota administracinė našta:
<table>
<tr><th>Eil. Nr.</th><th>Informacinis įpareigojimas</th><th>Vykdymo veiksmas</th><th>Tikslinė grupė</th><th>Kilmė</th><th>Administracinė našta</th></tr>
<tr><td rowspan="2">1.</td><td rowspan="2">iešai skelbti paslaugų gavėjams rekomendacijas apie priemones kibernetiniam saugumui užtikrinti naudojantis jūsų teikiamomis paslaugomis</td><td>informacijos rinkimas, apdorojimas ir skelbimas</td><td rowspan="2">elektroninės informacijos prieglobos paslaugų teikėjai</td><td rowspan="2">Kibernetinio saugumo įstatymas</td><td>429.717,75 Lt</td></tr>
<tr><td>įrangos, paslaugų pirkimas</td><td>78.120,00 Lt</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>507.837,75 Lt</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">teikti Ryšių reguliavimo tarnybai informaciją apie kibernetinius incidentus ir taikytas šių incidentų valdymo priemones bei techninę informaciją, reikalingą vertinti elektroninės informacijos prieglobos paslaugų kibernetinio saugumo būseną</td><td>informacijos rinkimas, apdorojimas ir teikimas</td><td rowspan="2">elektroninės informacijos prieglobos paslaugų teikėjai</td><td rowspan="2">Kibernetinio saugumo įstatymas</td><td>2.980.849,38 Lt</td></tr>
<tr><td>įrangos, paslaugų pirkimas</td><td>78.120,00 Lt</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>3.058.969,38 Lt</td></tr>
<tr><td>3</td><td>teikti Valstybinei duomenų apsaugos inspekcijai informaciją apie kibernetinius</td><td>informacijos rinkimas, apdorojimas ir teikimas</td><td>elektroninės informacijos prieglobos paslaugų</td><td>Kibernetinio saugumo įstatymas</td><td>378.945,00 Lt</td></tr>
</table>
</td></tr>
</table>

		incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones	įrangos, paslaugų pirkimas	teikėjai		78.120,00 Lt
						457.065,00 Lt
	4	teikti policijai informaciją, reikalingą kibernetinių incidentų, turinčių nusikalstamos veikos požymių, prevencijai ir tyrimui.	informacijos rinkimas, apdorojimas ir teikimas	elektroninės informacijos prieglobos paslaugų teikėjai	Kibernetinio saugumo įstatymas	442.614,38 Lt
			įrangos, paslaugų pirkimas			78.120,00 Lt
						520.734,38 Lt
						4.544.606,50 Lt
	5	viešai skelbti paslaugų gavėjams rekomendacijas apie priemones kibernetiniam saugumui užtikrinti naudojantis jūsų teikiamomis paslaugomis	informacijos rinkimas, apdorojimas ir skelbimas	viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai	Kibernetinio saugumo įstatymas	733.060,80 Lt
			įrangos, paslaugų pirkimas			257.538,39 Lt
						990.599,19 Lt
	6	teikti Ryšių reguliavimo tarnybai informaciją apie kibernetinius incidentus ir taikytas šių incidentų valdymo priemones bei techninę informaciją, reikalingą vertinti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų kibernetinio saugumo būseną	informacijos rinkimas, apdorojimas ir teikimas	viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai	Kibernetinio saugumo įstatymas	10.404.965,00 Lt
			įrangos, paslaugų pirkimas			839.507,78 Lt
						11.244.472,78 Lt
	7	teikti Valstybinei duomenų apsaugos inspekcijai informaciją apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones	informacijos rinkimas, apdorojimas ir teikimas	viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai	Kibernetinio saugumo įstatymas	5.825.940,00 Lt
			įrangos, paslaugų pirkimas			233.538,55 Lt
						6.059.478,55 Lt
	8	teikti policijai informaciją, reikalingą kibernetinių incidentų, turinčių nusikalstamos veikos požymių, prevencijai ir tyrimui.	informacijos rinkimas, apdorojimas ir teikimas	viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai	Kibernetinio saugumo įstatymas	2.971.613,25 Lt
			įrangos, paslaugų pirkimas			233.538,55 Lt
						3.205.151,80 Lt
						21.499.702,32 Lt
					Administracinė našta, iš viso:	**26.044.308,82 Lt**
Poveikis ekonomikai	***Status quo*** Neįmanoma įvertinti, kokią žalą ūkio subjektai patirtų, jei esama padėtis nesikeistų. Galima tik numanyti, kad žala nuolat didėtų, nes reguliariai auga kibernetinių incidentų mastai, atakuojamų ūkio subjektų kiekis. Be to, kiekvieno kibernetinio incidento atveju galima patirti žala yra skirtinga, kadangi, kaip jau					

	minėta anksčiau, žala priklauso ne tik nuo subjekto, kuriame įvyko incidentas, bet ir, koks incidento tipas, mastas ar trukmė. ***1-oji ir 2 alternatyvos***. Abiejų alternatyvų atveju Lietuvoje būtų sustiprintas kibernetinis saugumas. Stabilumo ir saugumo kibernetinėje erdvėje užtikrinimas teigiamai veikia šalies ekonomiką: pagreitinamas ir atpiginamas paslaugų teikimas, efektyviai komunikuojamų piliečių, ūkio subjektų ir valdžios veiksmai gerina šalies ūkio produktyvumą. Verslo subjektai, teikiantys elektroninės informacijos prieglobos paslaugas (šiuo metu jų yra apie 350 subjektų), viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų (100 subjektų) ir ypatingos svarbos informacinės infrastruktūros valdytojai (apie 50 subjektų) turės atitikti minimalius jiems nustatytus kibernetinio saugumo reikalavimus. Įgyvendinant nustatytus reikalavimus, verslo subjektams neturėtų reikti dalį investicijų skirti kibernetinio saugumo užtikrinimo priemonėms diegti. Nustatomi reikalavimai bus proporcingi įmonės teikiamų paslaugų apimčiai, t. y. mažoms ir didelėms įmonėms, teikiančioms tą pačią paslaugą, reikalavimai skirsis. Taip pat tikėtina, kad verslo subjektai, kuriems būtų taikomi didesni reikalavimai, rūpindamiesi savo reputacija ir teikiamų paslaugų kokybe, bus sudiegę geresnes kibernetinio saugumo užtikrinimo priemones, nei bus nustatyta reikalavimuose.
Poveikis viešojo valdymo sistemai	***Status quo*** Jei nebus imtasi jokių priemonių, poveikio viešojo valdymo sistemai nebus. ***1-oji alternatyva*** Įgyvendinant alternatyvą, bus užtikrintas viešojo administravimo subjektų, valdančių valstybės informacinius išteklius, teikiamų el. paslaugų prieinamumas ir saugumas. Kitos įtakos viešojo valdymo procesams įgyvendinama alternatyva neturės. Įgyvendinant projektą reikės įsteigti naują instituciją, Nacionalinį kibernetinio saugumo centrą, Krašto apsaugos ministerijos reguliavimo srityje. Nacionalinis kibernetinio saugumo centras turės būti įsteigtas iki įsigalios Kibernetinio saugumo įstatymas. Nacionalinis kibernetinio saugumo centras atliks šias funkcijas: • rengs ir tvirtins informacijos apie kibernetinius incidentus ir taikytas šių incidentų valdymo priemones pateikimo Nacionaliniam kibernetinio saugumo centrui tvarką ir sąlygas; • rengs ir tvirtins organizacinius ir techninius reikalavimus elektroninės informacijos prieglobos paslaugų saugumui ir vientisumui užtikrinti; • rengs ir tvirtins techninės informacijos, reikalingos vertinti viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir (arba) elektroninės informacijos prieglobos paslaugų kibernetinio saugumo būseną, pateikimo Nacionaliniam kibernetinio saugumo centrui tvarką ir sąlygas; • atliks viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų interneto prieigos tinklų infrastruktūros vientisumo tyrimus; • atliks viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir (arba) elektroninės informacijos prieglobos paslaugų kibernetinio saugumo būsenos tyrimus;

	• duos privalomus nurodymus ir nustatys nurodymų įvykdymo terminą viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams ir (arba) elektroninės informacijos prieglobos paslaugų teikėjams; • pagal savo kompetenciją rengs ir teiks siūlymus krašto apsaugos ministrui dėl organizacinių ir techninių kibernetinio saugumo reikalavimų valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai; • vykdys valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams stebėseną; • rengs tipinius kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus; • teiks konsultacijas ir rekomendacijas kibernetinio saugumo klausimais valstybės informacinių išteklių valdytojams, ypatingos svarbos infrastruktūros valdytojams, viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų teikėjams; • analizuos nacionalinę kibernetinio saugumo situaciją ir rengs nacionalinio kibernetinio saugumo būklės ataskaitas; • rengs ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus; • valdys kibernetinio saugumo informacinį tinklą; • vykdys informacijos sklaidą kibernetinio saugumo klausimais; • atliks kitas Lietuvos Respublikos teisės aktų numatytas funkcijas kibernetinio saugumo užtikrinimo srityje. Kibernetinio saugumo politikos formavime ir įgyvendinime pagal kompetenciją taip pat dalyvaus Policijos departamentas prie Vidaus reikalų ministerijos ir Valstybinė duomenų apsaugos inspekcija. Įgyvendinant alternatyvą, į Krašto apsaugos ministeriją turėtų būti perkeltos pareigybės iš kitų institucijų, formuojančių, dalyvaujančių formuojant kibernetinio saugumo politiką, t.y. Ryšių reguliavimo tarnybos ir Vidaus reikalų ministerijos. Į Nacionalinį kibernetinio saugumo centrą turėtų būti perkeltos pareigybės, atsakingos už kibernetinį saugumą, iš institucijų, dalyvaujančių kibernetinio saugumo užtikrinime, t. y. Ryšių reguliavimo tarnybos, Informatikos ir ryšių departamento prie Vidaus reikalų ministerijos. Atitinkamai į Krašto apsaugos ministeriją ir Nacionalinį kibernetinio saugumo centrą iki įstatymo įsigaliojimo dienos bus perkeltos ir kitų institucijų atliekamos funkcijos, susijusios su kibernetiniu saugumu. Be jau Nacionaliniam kibernetinio saugumo centrui nustatytų naujų funkcijų, taip pat Krašto apsaugos ministerijai bus nustatyta nauja, papildoma funkcija – formuoti kibernetinio saugumo politiką ir koordinuoti ir kontroliuoti jos įgyvendinimą. Įgyvendinant alternatyvą į Nacionalinį kibernetinio saugumo centrą reikės priimti naujų valstybės tarnautojų. Tarnautojų poreikis išdėstytas poveikio valstybės finansams skiltyje. Tarnautojai turės būti priimami vykdyti Kibernetinio saugumo įstatyme nustatytas funkcijas, todėl jų poreikis būtinas iki tol, kol reikalingas nustatytų funkcijų vykdymas. Valstybės tarnautojai atsakingi už kibernetinio saugumo politikos formavimą ir įgyvendinimą turės nuolat dalyvauti kvalifikacijos kėlimo kursuose, seminaruose ir taip reguliariai tobulinti kompetencijas, reikalingas kibernetiniam

	saugumui užtikrinti. ***2-oji alternatyva*** Įgyvendinant alternatyvą, bus užtikrintas viešojo administravimo subjektų, valdančių valstybės informacinius išteklius, teikiamų el. paslaugų prieinamumas ir saugumas. Kitos įtakos viešojo valdymo procesams įgyvendinama alternatyva neturės. Įgyvendinant projektą reikės įsteigti naują instituciją, Nacionalinį kibernetinio saugumo centrą, Krašto apsaugos ministerijos reguliavimo srityje. Nacionalinis kibernetinio saugumo centras turės būti įsteigtas iki įsigalios Kibernetinio saugumo įstatymas. Nacionalinis kibernetinio saugumo centras atliks šias funkcijas: • pagal savo kompetenciją rengs ir teiks siūlymus krašto apsaugos ministrui dėl organizacinių ir techninių kibernetinio saugumo reikalavimų valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai; • vykdys valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams stebėseną; • rengs tipinius kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus; • teiks konsultacijas ir rekomendacijas kibernetinio saugumo klausimais valstybės informacinių išteklių valdytojams ir ypatingos svarbos infrastruktūros valdytojams; • analizuos nacionalinę kibernetinio saugumo situaciją ir rengs nacionalinio kibernetinio saugumo būklės ataskaitas; • rengs ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus; • valdys kibernetinio saugumo informacinį tinklą; • vykdys informacijos sklaidą kibernetinio saugumo klausimais; • atliks kitas Lietuvos Respublikos teisės aktų numatytas funkcijas kibernetinio saugumo užtikrinimo srityje. Įgyvendinant alternatyvą nereikės pertvarkyti ar likviduoti esamų valstybės institucijų, taip pat nebus perskirstomos valstybės institucijų funkcijos. Be jau Nacionaliniam kibernetinio saugumo centrui nustatytų naujų funkcijų, taip pat Krašto apsaugos ministerijai bus nustatyta nauja, papildoma funkcija – formuoti kibernetinio saugumo politiką ir koordinuoti ir kontroliuoti jos įgyvendinimą, Vidaus reikalų ministerijai – pagal kompetenciją dalyvauti formuojant kibernetinio saugumo politiką ir Ryšių reguliavimo tarnyba papildomai turės atlikti šias funkcijas: • rengti ir tvirtinti informacijos apie kibernetinius incidentus ir taikytas šių incidentų valdymo priemones pateikimo Ryšių reguliavimo tarnybai tvarką ir sąlygas; • rengti ir tvirtinti organizacinius ir techninius reikalavimus elektroninės informacijos prieglobos paslaugų saugumui ir vientisumui užtikrinti; • rengti ir tvirtinti techninės informacijos, reikalingos vertinti viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir (arba) elektroninės informacijos prieglobos paslaugų kibernetinio saugumo būseną, pateikimo Ryšių reguliavimo

	tarnybai tvarką ir sąlygas; • atlikti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų interneto prieigos tinklų infrastruktūros vientisumo tyrimus; • atlikti viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir (arba) elektroninės informacijos prieglobos paslaugų kibernetinio saugumo būsenos tyrimus; • duoti privalomus nurodymus ir nustatys nurodymų įvykdymo terminą viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams ir (arba) elektroninės informacijos prieglobos paslaugų teikėjams. Kibernetinio saugumo politikos formavime ir įgyvendinime pagal kompetenciją taip pat dalyvaus Policijos departamentas prie Vidaus reikalų ministerijos ir Valstybinė duomenų apsaugos inspekcija. Įgyvendinant alternatyvą į Nacionalinį kibernetinio saugumo centrą reikės priimti naujų valstybės tarnautojų. Tarnautojų poreikis išdėstytas poveikio valstybės finansams skiltyje. Tarnautojai turės būti priimami vykdyti Kibernetinio saugumo įstatyme nustatytas funkcijas, todėl jų poreikis būtinas iki tol, kol reikalingas nustatytų funkcijų vykdymas. Valstybės tarnautojai atsakingi už kibernetinio saugumo politikos formavimą ir įgyvendinimą turės nuolat dalyvauti kvalifikacijos kėlimo kursuose, seminaruose ir taip reguliariai tobulinti kompetencijas, reikalingas kibernetiniam saugumui užtikrinti.

Kiti poveikio vertinimo aspektai	***Status quo***	**1-oji alternatyva**	**2-oji alternatyva**
Teisinei sistemai	Kibernetinio saugumo sritis lieka teisiškai nereglamentuota	Kibernetinio saugumo įstatymas neprieštarauja Lietuvos Respublikos Konstitucijai, įstatymams ir įstatymų lydimiesiems aktams, kitiems teisės aktams. Kibernetinio saugumo įstatymas nekartoja jau įtvirtinto reglamentavimo. Priėmus Kibernetinio saugumo įstatymą neatsiras teisės normų (teisinio reguliavimo) kolizijos, konkurencijos, taip pat nesidubliuos institucijų funkcijos. Kibernetinio saugumo įstatymu nėra perkeliami Europos Sąjungos teisės aktai į nacionalinę teisę. Kibernetinio saugumo įstatyme nustatytos priemonės yra proporcingos siekiamam tikslui ir būtinos teisiniam reguliavimui tobulinti. Atsižvelgdami į kibernetinio saugumo aktualumą ir svarbą, manome, kad tinkamai nustatyti įsigaliojimo terminai. Kibernetinio saugumo įstatymas nekliudys	

Kiti poveikio vertinimo aspektai	*Status quo*	1-oji alternatyva	2-oji alternatyva
		sudaryti lygias galimybes visiems asmenims nepaisant jų tautybės, lyties, įsitikinimų ginti savo teises, teisėtus interesus ir siekti teisingumo. Manome, kad Kibernetinio saugumo įstatyme pasirinkti tinkami reguliavimo metodai. Kibernetinio saugumo įstatyme numatytos proporcingos sankcijos už reikalavimų nesilaikymą, paaiškinimai dėl siūlomos administracinės nuobaudos tipo ir dydžio pateikti aiškinamajame rašte. Už to paties reikalavimo nesilaikymą yra numatyta taikyti pakartotinę didesnę sankciją, jei asmuo per nustatytą protingą terminą neįvykdė keliamų reikalavimų. Numatomos sankcijos diferencijuojamos. Nustatyta tinkama reikalavimų laikymosi ir priežiūros kontrolė.	
Kriminogeninei situacijai	Nusikaltimų kibernetinėje erdvėje prevencija ir tyrimai vykdomi pagal galiojančius teisės aktus.	Kibernetinio saugumo įstatymo projekte numatyta vykdyti kibernetinių incidentų, turinčių nusikalstamos veikos požymių, prevenciją, todėl turėtų sumažėti nusikalstamos veikos kibernetinėje erdvėje. Kibernetinio saugumo įstatymas nepaveiks teisėsaugos ir kitų baudžiamojo teisingumo institucijų veiklos efektyvumo.	

Alternatyvų palyginimas

Status quo situacija nėra tinkama, kadangi tobulėjant informacijos ir ryšių technologijoms yra būtinas tinkamas kibernetinio saugumo užtikrinimas, kadangi didėjančios kibernetinės grėsmės gali turėti labai didelį poveikį valstybės funkcijų vykdymui, viešajai tvarkai ar nacionaliniam saugumui. Be to, valstybė ateityje gali patirti didelę žalą nuo kibernetinių incidentų, ypač tų, kurie vyksta ypatingos svarbos informacinėje infrastruktūroje.
1-osiosios ir 2-osios alternatyvų palyginimas:

1-alternatyva	2-alternatyva
Kibernetinio saugumo politiką formuos Krašto apsaugos ministerija, dalyvaus formuojant politiką ir ją įgyvendins Nacionalinis kibernetinio saugumo centras. Kibernetinio saugumo politikos formavime ir įgyvendinime pagal kompetenciją taip pat dalyvaus	Kibernetinio saugumo politiką formuos Krašto apsaugos ministerija, politikos formavime dalyvaus Vidaus reikalų ministerija, Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija ir Policijos

Policijos departamentas prie Vidaus reikalų ministerijos ir Valstybinė duomenų apsaugos inspekcija.	departamentas prie Vidaus reikalų ministerijos, o pagal kompetenciją įgyvendins Ryšių reguliavimo tarnyba, Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija ir Policijos departamentas prie Vidaus reikalų ministerijos.
Kibernetinio saugumo užtikrinimo sistemos kūrimas ir kibernetinių incidentų valdymo sistemos kūrimas užtruktų ilgiau, nes viską reikėtų pradėti nuo nulio, atsisakant šiuo metu esamo įdirbio.	Kibernetinio saugumo užtikrinimo sistemos kūrimas ir kibernetinių incidentų valdymo sistemos kūrimas užtruktų mažiau laiko ir pareikalautų mažesnių organizacinių pertvarkų, nes būtų išnaudojama ir praplečiama esama sistema.
Bendras poveikis valstybės finansams – 19189,1 tūkst. Lt.	Bendras poveikis valstybės finansams – 12703,7 tūkst. Lt.
Administracinė našta – 26044,3 tūkst. Lt.	Administracinė našta – 26044,3 tūkst. Lt.
Didelė organizacinė pertvarka, naujos institucijos steigimas, funkcijų ir pareigybių persiskirstymas ir naujų funkcijų ir pareigybių nustatymas Nacionaliniam kibernetinio saugumo centrui.	Organizacinės institucijų pertvarkos nėra, įsteigiama nauja institucija. Naujos kibernetinio saugumo funkcijos paskirstomos pagal kompetenciją šiuo metu su kibernetiniu saugumu dirbančiai institucijai (Ryšių reguliavimo tarnybai) ir įsteigtam Nacionaliniam kibernetinio saugumo centrui.

Siūloma alternatyva ir jos įgyvendinimo būdai

Atsižvelgiant į tai, kas išdėstyta, kaip efektyviausią ir reikalaujančią mažiausiai sąnaudų, siūlome pasirinkti 2-ąją alternatyvą, taip pat rengti Lietuvos Respublikos kibernetinio saugumo įstatymo projektą bei Lietuvos Respublikos administracinių teisės pažeidimų kodekso, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo bei kitų reikalingų įstatymų pakeitimo įstatymus.

Kita svarbi informacija

Numatomos konsultacijos su suinteresuotomis institucijomis ir visuomene skelbiant įstatymo projektą Lietuvos Respublikos Seimo teisės aktų informacinėje sistemoje (TAIS).

Informacija apie asmenį ir instituciją, atsakingą už poveikio vertinimą

Vardas ir pavardė	Tomas Stamulis

Pareigos	patarėjas
Institucija (padalinys)	Lietuvos Respublikos vidaus reikalų ministerijos Elektroninės valdžios politikos skyrius
Telefono numeris ir elektroninio pašto adresas	8 5 271 7356 tomas.stamulis@vrm.lt