LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO NR. XII-1428 1, 2, 6, 8, 9, 13 STRAIPSNIŲ, V SKYRIAUS PAVADINIMO, PRIEDO PAKEITIMO IR ĮSTATYMO PAPILDYMO 17 STRAIPSNIU IR VI SKYRIUMI ĮSTATYMO IR LIETUVOS RESPUBLIKOS ADMINISTRACINIŲ NUSIŽENGIMŲ KODEKSO PAPILDYMO 480^1 STRAIPSNIU IR 589 STRAIPSNIO BEI PRIEDO PAKEITIMO ĮSTATYMO PROJEKTŲ AIŠKINAMASIS RAŠTAS

1. Įstatymų projektų rengimą paskatinusios priežastys, parengtų projektų tikslai ir uždaviniai

Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 1, 2, 6, 8, 9, 13 straipsnių, V skyriaus pavadinimo, priedo pakeitimo ir įstatymo papildymo 17 straipsniu ir VI skyriumi įstatymo projekto (toliau – KSĮ pakeitimo projektas) ir Lietuvos Respublikos administracinių nusižengimų kodekso papildymo 480^1 straipsniu ir 589 straipsnio bei priedo pakeitimo įstatymo projekto (toliau – ANK pakeitimo projektas) rengimo priežastys yra:

1) 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (toliau – Kibernetinio saugumo aktas), kuriuo nustatoma Europos kibernetinio saugumo sertifikavimo sistema ir numatoma pareiga valstybėms narėms paskirti nacionalinę kibernetinio saugumo sertifikavimo instituciją;

2) atsakingo ryšių ir informacinių sistemų spragų (toliau – spraga) atskleidimo reglamentavimo poreikis;

3) tikslesnio techninių kibernetinio saugumo priemonių apibrėžimo poreikis;

4) reglamentavimo, susijusio su Kibernetinio saugumo informaciniu tinklu, tikslinimas.

1.1. Dėl Kibernetinio saugumo akto

Kibernetinio saugumo aktu sukuriama Europos Sąjungos masto sertifikavimo sistema ir įsteigiama Europos Sąjungos kibernetinio saugumo agentūra, kuri modernizuos ir perims veiklą iš dabartinės Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA). Kibernetinio saugumo aktu numatoma, kad Europos Komisija galės priimti įgyvendinamuosius aktus, kuriuose būtų numatytas informacinių ir ryšių technologijų (toliau – IRT) produktų, procesų ir paslaugų Europos kibernetinio saugumo sertifikavimo schemos. Patvirtinus Europos kibernetinio saugumo sertifikavimo schemą IRT produktų gamintojai arba IRT paslaugų ar procesų teikėjai turėtų galimybę teikti prašymą jų pasirinktai atitikties vertinimo įstaigai, apibrėžtai 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamente (EB) Nr. 765/2008, nustatančiame su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus ir panaikinančiame Reglamentą (EEB) Nr. 339/93 (toliau − Reglamentas (EB) Nr. 765/2008), sertifikuoti jų IRT produktus, paslaugas ar procesus. Atitikties vertinimo įstaigas akredituotų nacionalinė akreditacijos įstaiga, Lietuvoje tai yra Nacionalinis akreditacijos biuras. Kibernetinio saugumo sertifikavimas būtų savanoriškas, nebent Europos Sąjungos ar valstybės narės teisėje būtų numatyta kitaip.

Kibernetinio saugumo aktas įsigaliojo 2019 m. gegužės mėnesį ir yra tiesioginio taikymo teisės aktas, tačiau su valstybėms narėms numatomais įpareigojimais susijusios nuostatos įsigalioja

2021 m. birželio 28 d., todėl nacionalinės teisės pakeitimai turi būti atlikti iki šių nuostatų įsigaliojimo.

Kibernetinio saugumo akto 58 straipsnio 1 dalyje yra numatytas įpareigojimas valstybėms narėms paskirti vieną nacionalinę kibernetinio saugumo sertifikavimo instituciją arba kelias tokias institucijas arba, sudarius susitarimą su kita valstybe nare, paskirti kitoje valstybėje narėje įsisteigusią nacionalinę kibernetinio saugumo sertifikavimo instituciją arba kelias nacionalines kibernetinio saugumo sertifikavimo institucijas būti atsakinga (-omis) už priežiūros užduotis paskyrusioje valstybėje narėje.

Kibernetinio saugumo akto 65 straipsnyje yra numatytas įpareigojimas valstybėms narėms nustatyti taisykles, kuriomis reglamentuojamos už Europos kibernetinio saugumo sertifikavimo schemų nuostatų pažeidimus taikytinos veiksmingos, proporcingos ir atgrasomosios sankcijos, ir imtis visų reikiamų priemonių, kad užtikrintų jų įgyvendinimą.

Šiuo aspektu KSĮ pakeitimo ir ANK pakeitimo projektų tikslas yra įgyvendinti Kibernetinio saugumo akto įpareigojimus, o uždaviniai:

1) paskirti nacionalinę kibernetinio saugumo sertifikavimo instituciją;

2) nustatyti nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas;

3) numatyti atsakomybę už kibernetinio saugumo sertifikavimo pareigų atlikimo pažeidimus.

1.2. Dėl atsakingo spragų atskleidimo reglamentavimo

Nacionalinės kibernetinio saugumo strategijos, patvirtintos Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Kibernetinio saugumo strategija) 37 punkte nurodoma, kad spragų ieško asmenys, turintys skirtingų tikslų, tačiau, siekiant atsakingumo atskleidžiant spragas, svarbu sudaryti galimybę saugumo spragą suradusiam ir norinčiam jį ištaisyti asmeniui bendradarbiauti su kibernetinio saugumo subjektais, kurių ryšių ir informacinėse sistemose spraga buvo atskleista. Kibernetinio saugumo subjektai, nustatę ir viešai paskelbę spragų atskleidimo tvarką, apsisaugotų nuo kibernetinių incidentų galimos žalos arba ją labai sumažintų. Spragų atskleidimo tvarkos nustatymas ir viešas paskelbimas prisidėtų prie valstybės kibernetinio saugumo užtikrinimo ir sudarytų daugiau viešojo ir privataus sektorių bendradarbiavimo galimybių.

SANS instituto duomenimis, spragą aptikęs asmuo turi keturis pasirinkimus:

1) neatskleidimas (angl. *nondisclosure*) – informacija apie spragą neperduodama niekam. Spragą radęs asmuo informaciją apie šią spragą pasilieka sau;

2) visiškas atskleidimas (angl. *full disclosure*) – informacija apie spragą atskleidžiama plačiajai auditorijai, nepaliekant kibernetinio saugumo subjektui, kurio sistemose spraga buvo aptikta, pakankamai laiko spragai pašalinti;

3) ribotas atskleidimas (angl. *limited disclosure*) – informacija apie spragą pateikiama tik tam tikroms suinteresuotoms šalims, pvz., Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – Nacionalinis kibernetinio saugumo centras);

4) atsakingas atskleidimas (angl. *responsible disclosure*) – informacijos apie spragą atskleidimas koordinuojamas su kibernetinio saugumo subjektu, kurio sistemose spraga buvo aptikta.[1]

Remiantis Pasaulinio kibernetinio ekspertinių žinių forumo rekomendacijomis, spragų atskleidimo procesą palengvinti gali atsakingo spragų atskleidimo tvarkos taikymas arba patikimos valstybinės institucijos dalyvavimas. Atsakingo spragų atskleidimo taisyklės yra dokumentas, kurį paviešinęs subjektas apibrėžia atsakingo spragų atskleidimo procesą bei nustato šiame procese

[1]https://www.sans.org/reading-room/whitepapers/threats/defineresponsible-disclosure-932.

dalyvaujančių suinteresuotų šalių teises ir pareigas. Vadovaudamasis atsakingo spragų atskleidimo taisyklėmis, spragą aptikęs asmuo galėtų apie ją pranešti organizacijai, kurios sistemose buvo aptikta spraga, ir koordinuoto dvišalio proceso metu užtikrinti šios spragos pašalinimą. Kitu atveju minėtas asmuo taip pat galėtų kreiptis į atsakingo atskleidimo tvarką viešinančią patikimą valstybės instituciją, pvz., Nacionalinį kibernetinio saugumo centrą, kuris, atlikdamas tarpininko vaidmenį, dalyvautų trišaliame atsakingo atskleidimo procese, kurio metu spraga būtų pašalinta.

Kadangi Lietuvos Respublikos teisės aktuose nėra formalaus atsakingo spragų atskleidimo aprašymo, o šalies kibernetinio saugumo subjektai nenustato atsakingo spragų atskleidimo tvarkos, spragas aptikę asmenys nėra tikri, ar jų rasta spraga bus pašalinta, bei susiduria su klausimais dėl savo teisinės padėties. Apie aptiktą spragą gali būti pasirinkta pranešti viešai arba jos neatskleisti visai. Asmuo, pasirinkęs visiško atskleidimo metodą, ne tik nesuteikia kibernetinio saugumo subjektui galimybės pašalinti spragą, bet ir rizikuoja užsitraukti baudžiamąją atsakomybę. Tačiau jeigu informacija apie spragą lieka paslaptyje, tikėtina, kad spraga liks nepašalinta ir ją išnaudos piktavaliai. Abiem atvejais tikėtina, kad bus padaryta žala kibernetinio saugumo subjekto reputacijai ir piktavaliams bus palikta galimybė išnaudoti spragą.

Papildomai pažymėtina, kad Lietuvos Respublikos baudžiamojo kodekso XXX skyriaus nuostatos (ypač 198 ir 198^1 straipsniai) yra suformuluotos taip, kad spragų iš esmės neįmanoma aptikti formaliai neatlikus teisės pažeidimo, neatsižvelgiant į atliekamų veiksmų pavojingumą ar intensyvumą. Tai reiškia, kad be išankstinio ryšių ir informacinės sistemos valdytojo leidimo bet koks spragos aptikimas būtų traktuojamas kaip nusikalstama veika, todėl asmenys, aptikę spragą, paprastai pasirenka ją laikyti paslaptyje.

Atsižvelgiant į tai, kas išdėstyta, siūlomas Lietuvos Respublikos kibernetinio saugumo įstatymo pakeitimas, kurio tikslas – nustatyti atsakingo spragų atskleidimo modelį, o uždaviniai yra:

1) nustatyti sąlygas, kurių laikantis būtų galima teisėtai ieškoti spragų;
2) pavesti krašto apsaugos ministrui tvirtinti nacionalinės spragų atskleidimo tvarkos aprašą.

1.3. Dėl techninių kibernetinio saugumo priemonių

Kibernetinio saugumo įstatymo 8 straipsnio 2 dalies 8 punkte yra numatyta Nacionalinio kibernetinio saugumo centro pareiga diegti ir valdyti technines kibernetinio saugumo priemones valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose, o Kibernetinio saugumo įstatymo 6 straipsnio 6 punkte numatyta Krašto apsaugos ministerijos pareiga tvirtinti techninių kibernetinio saugumo priemonių diegimo planą, nustatyti jų diegimo ir valdymo tvarką.

Nepaisant to, Kibernetinio saugumo įstatyme nėra apibrėžiamos techninės kibernetinio saugumo priemonės, todėl susidaro situacija, kad Nacionalinis kibernetinio saugumo centras turi teisę diegti kibernetinio saugumo subjektų ryšių ir informacinėse sistemose teisiškai neapibrėžtas technines kibernetinio saugumo priemones.

Atsižvelgiant į tai, siūlomas Kibernetinio saugumo įstatymo pakeitimas, kurio tikslas – tikslinti su techninėmis kibernetinio saugumo priemonėmis susijusį teisinį reguliavimą, o nustatomas uždavinys – nustatyti pareigą Krašto apsaugos ministrui tvirtinti techninių kibernetinio saugumo priemonių sąrašą.

1.4. Dėl Kibernetinio saugumo informacinio tinklo

Kibernetinio saugumo įstatymo 13 straipsnis nustato Kibernetinio saugumo informacinio tinklo paskirtį, jo naudojimo sąlygas ir jame tvarkomų asmens duomenų apimtį.

Kibernetinio saugumo informacinis tinklas naudojamas vykdant ir kitas Nacionalinio kibernetinio saugumo centro funkcijas, tačiau šios funkcijos nenurodomos Kibernetinio saugumo informacinio tinklo paskirtyje. Be to, Kibernetinio saugumo informaciniame tinkle yra saugomi

duomenys, susiję su kibernetinio saugumo subjektų ryšių ir informacinėse sistemose įvykusiais kibernetiniais incidentais. Tokio pobūdžio informacija yra ypač jautri kibernetinio saugumo subjektams ir neturėtų būti teikiama tretiesiems asmenims.

Atsižvelgiant į tai, kas išdėstyta, siūlomas Lietuvos Respublikos kibernetinio saugumo įstatymo pakeitimas, kurio tikslas – tiksliau aprašyti Kibernetinio saugumo informacinį tinklą, o uždaviniai yra:

1) patikslinti Kibernetinio saugumo informacinio tinklo paskirtį;
2) nustatyti Kibernetinio saugumo informacinio tinklo duomenų teikimo sąlygas.

2. Įstatymų projektų iniciatoriai (institucija, asmenys ar piliečių įgalioti atstovai) ir rengėjai

Įstatymų projektus rengė Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų politikos grupės (grupės vadovas Jonas Skardinskas, tel. 8 706 80 800, el. p. jonas.skardinskas@kam.lt) patarėja Sigita Laurinčiukaitė (tel. 8 706 80 804, el. p. sigita.laurinciukaite@kam.lt) ir Krašto apsaugos ministerijos Teisės departamento (direktorė Judita Nagienė, tel. (8 5) 273 5545, el. p. judita.nagiene@kam.lt) Teisėkūros skyriaus (skyriaus vedėjas Tomas Vainius, tel. (8 5) 273 5563, el. p. tomas.vainius@kam.lt) patarėjas kpt. Mantas Keliotis (tel. (8 5) 273 5597, el. p. mantas.keliotis@kam.lt). KSĮ pakeitimo projekto dalis, susijusi su spragų atskleidimu, parengta bendradarbiaujant su projekto „Kurk Lietuvai“ projekto vadovu Žygimantu Robertu Tamošausku.

3. Kaip šiuo metu yra reguliuojami įstatymų projektuose aptarti teisiniai santykiai

3.1. Dėl Kibernetinio saugumo akto

Kibernetinio saugumo įstatymo II skyriuje nurodomos kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos ir įtvirtinami jų įgaliojimai. Šiuo metu Kibernetinio saugumo įstatyme nėra nustatyta, kokia valstybinė institucija atlieka Kibernetinio saugumo akte nurodytos nacionalinės kibernetinio saugumo institucijos funkcijas ir turi atitinkamus įgaliojimus.

Kibernetinio saugumo akto 65 straipsnis nustato pareigą valstybėms narėms nustatyti taisykles, kuriomis reglamentuojamos už Kibernetinio saugumo akto III antraštinės dalies ir Europos kibernetinio saugumo sertifikavimo schemų nuostatų pažeidimus taikytinos sankcijos, ir imtis visų reikiamų priemonių, kad užtikrintų jų įgyvendinimą. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomosios. Administracinių nusižengimų kodekso 479 ir 480 straipsniai nustato sankcijas už Lietuvos Respublikos kibernetinio saugumo įstatymo nuostatų ir nustatytų pareigų atlikimo pažeidimą, tačiau galiojantis teisinis reguliavimas neapima sankcijų už Kibernetinio saugumo akte numatytus pažeidimus.

3.2. Dėl atsakingo spragų atskleidimo reglamentavimo

Šiuo metu nacionaliniu mastu spragų atskleidimo tvarka nėra nustatyta, o savarankiškai nustatytą atsakingo spragų atskleidimo tvarką Lietuvoje taiko tik pavienės organizacijos.

3.3. Dėl techninių kibernetinio saugumo priemonių

Kibernetinio saugumo įstatymo 8 straipsnio 2 dalies 8 punkte yra numatyta Nacionalinio kibernetinio saugumo centro pareiga diegti ir valdyti technines kibernetinio saugumo priemones valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose, o 6 straipsnio 6 punkte numatyta Krašto apsaugos ministerijos pareiga tvirtinti techninių kibernetinio saugumo priemonių diegimo planą, nustatyti jų diegimo ir valdymo tvarką, tačiau techninės kibernetinio saugumo priemonės nėra apibrėžiamos ir niekam nenumatoma pareiga tai padaryti.

3.4. Dėl Kibernetinio saugumo informacinio tinklo

Kibernetinio saugumo įstatymo 13 straipsnio 1 dalyje yra įtvirtina Kibernetinio saugumo informacinio tinklo paskirtis – dalytis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir Kibernetinio saugumo informacinio tinklo narių tarpusavio bendradarbiavimą kibernetinio saugumo srityje. Įstatyme nurodyta paskirtimi nėra atskleidžiama Kibernetinio saugumo informacinio tinklo sąsaja su techninėmis kibernetinio saugumo priemonėmis.

Vadovaujantis Kibernetinio saugumo informacinio tinklo nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2019 m. lapkričio 27 d. įsakymu Nr. V-998 „Dėl Kibernetinio saugumo informacinio tinklo nuostatų patvirtinimo“, 19 punktu, Kibernetinio saugumo informaciniame tinkle yra:

1) kaupiami techninėmis kibernetinio saugumo priemonėmis surinkti metaduomenys apie Kibernetinio saugumo informacinio tinklo narių ryšių ir informacinių sistemų komunikacijas;

2) surinkti metaduomenys yra apdorojami, nustatoma, kurie iš jų gali identifikuoti kibernetinių incidentų požymius, ir jie priskiriami kibernetinio incidento požymių indikatoriams;

3) pagal kibernetinio incidento požymių indikatorius, jų rinkinius ir surinktus metaduomenis automatiniu būdu ir (arba) retrospektyviai identifikuojami kibernetinių incidentų požymiai.

Kibernetinio saugumo įstatymo 15 straipsnyje nustatoma, kad kibernetinio saugumo politikos įgyvendinimo institucijos kibernetinio saugumo subjektų pateikta informacija, įskaitant ir konfidencialią, turi teisę keistis tik tiek, kiek tai yra būtina šių institucijų funkcijoms pagal kompetenciją atlikti, ir privalo užtikrinti gautos informacijos apsaugą, tačiau nėra aiškiai nurodoma, kad Kibernetinio saugumo informacinio tinklo duomenys yra konfidencialūs ir neteikiami tretiesiems asmenims.

4. Kokios siūlomos naujos teisinio reguliavimo nuostatos ir kokių teigiamų rezultatų laukiama

4.1. Dėl Kibernetinio saugumo akto

Kibernetinio saugumo įstatymo 1 straipsnio 1 dalį siūloma papildyti nuostata, kad Kibernetinio saugumo įstatymas nustato nacionalinę kibernetinio saugumo sertifikavimo instituciją ir jos įgaliojimus bei ryšių ir informacinių sistemų spragų paieškos ir pranešimo apie jas ir kibernetinius incidentus pagrindus.

Kibernetinio saugumo įstatymo 2 straipsnio 19 dalį siūloma papildyti nurodant, kad Europos kibernetinio saugumo sertifikavimo schemos, Europos kibernetinio saugumo sertifikato, akreditavimo ir atitikties vertinimo įstaigos sąvokos suprantamos taip, kaip jos apibrėžtos Kibernetinio saugumo akte.

Kibernetinio saugumo įstatymą siūloma papildyti VI skyriumi, kurio 18 straipsnio 1 dalis nustatytų, kad Nacionalinis kibernetinio saugumo centras vykdo Kibernetinio saugumo akte nustatytas nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas ir turi nacionalinės kibernetinio saugumo sertifikavimo institucijos įgaliojimus, 18 straipsnio 2 dalis nustatytų Nacionalinio kibernetinio saugumo centro funkcijas kibernetinio saugumo sertifikavimo srityje. VI skyriaus 19 straipsniu siūloma nustatyti principines papildomų įgaliojimų atitikties vertinimo įstaigoms teikimo, apribojimo ir sustabdymo, papildomų įgaliojimų apribojimo ir sustabdymo panaikinimo, papildomų įgaliojimų atšaukimo nuostatas. Atitikties vertinimo įstaigoms suteikiami įgaliojimai iš esmės tik papildytų atitikties vertinimo įstaigoms pagal Lietuvos Respublikos

atitikties vertinimo įstatymo, kurio nauja redakcija įsigalioja 2021 m. gegužės 1 d., suteikiamus akreditavimo pažymėjimus, todėl 19 straipsniu numatomą teisinį reguliavimą siūlytina nustatyti atsižvelgiant į nauja redakcija dėstomo Atitikties vertinimo įstatymo nuostatas. Atkreiptinas dėmesys, kad nauja redakcija dėstomame Atitikties vertinimo įstatyme nustatoma specifinė atitikties vertinimo įstaigų priežiūros samprata, todėl Lietuvos Respublikos viešojo administravimo įstatymas, ypač kiek tai susiję su licencijavimu ir ūkio subjektų veiklos priežiūra, taikomas tiek pat, kiek ir atliekant atitikties vertinimo įstaigų priežiūrą. VI skyriaus 20 straipsniu siūloma apibrėžti Nacionalinio kibernetinio saugumo centro vykdytinus kibernetinio saugumo sertifikavimo srities tyrimus ir jų atlikimo tvarką, terminus bei sprendimus, atlikus tyrimą. Tyrimai turėtų būti atliekami per kuo trumpesnį laiką, tačiau ne ilgiau nei per 4 mėnesius, su galimybe, atsižvelgiant į tyrimo sudėtingumą, terminą pratęsti 2 mėnesiais. Siūlomais pakeitimais būtų įgyvendinti Kibernetinio saugumo akto 58 straipsnio 1, 7 ir 8 dalių reikalavimai.

Vadovaudamasi Kibernetinio saugumo aktu, nacionalinė kibernetinio saugumo sertifikavimo institucija stebėtų, kaip atitinkamoje teritorijoje įsisteigę IRT produktų gamintojai arba IRT paslaugų ar procesų teikėjai vykdo su Europos Sąjungos atitikties pareiškimu susijusias pareigas, ir užtikrintų jų vykdymą (Kibernetinio saugumo akto 58 straipsnio 7 dalies b punktas), padėtų nacionalinėms akreditacijos įstaigoms vykdyti atitikties vertinimo įstaigų atliekamą stebėsenos ir priežiūros veiklą, teikdama joms ekspertines žinias ir atitinkamą informaciją (Kibernetinio saugumo akto 58 straipsnio 7 dalies c punktas), įgaliotų atitikties vertinimo įstaigas atlikti užduotis, kai tos įstaigos tenkina papildomus Europos kibernetinio saugumo sertifikavimo schemoje nustatytus reikalavimus (Kibernetinio saugumo akto 58 straipsnio 7 dalies e punktas), ir stebėtų svarbius pokyčius kibernetinio saugumo sertifikavimo srityje (Kibernetinio saugumo akto 58 straipsnio 7 dalies i punktas). Nacionalinė kibernetinio saugumo sertifikavimo institucija taip pat nagrinėtų fizinių ar juridinių asmenų pateiktus skundus, susijusius su tų institucijų išduotais Europos kibernetinio saugumo sertifikatais arba atitikties vertinimo įstaigų išduotais Europos kibernetinio saugumo sertifikatais, patvirtinančiais aukštą saugumo užtikrinimo lygį (Kibernetinio saugumo akto 58 straipsnio 7 dalies f punktas). Be to, nacionalinė kibernetinio saugumo sertifikavimo institucija turėtų bendradarbiauti su kitų valstybių narių nacionalinėmis kibernetinio saugumo sertifikavimo institucijomis ar kitomis valdžios institucijomis, be kita ko, dalydamosi informacija apie galimą IRT produktų, paslaugų ir procesų neatitiktį Kibernetinio saugumo akto arba konkrečių Europos kibernetinio saugumo sertifikavimo schemų reikalavimams (Kibernetinio saugumo akto 58 straipsnio 7 dalies h punktas).

Atsižvelgiant į Kibernetinio saugumo akto 58 straipsnio 7 dalies d punktą, 18 straipsnio 2 dalies 5 punkte nacionalinei kibernetinio saugumo sertifikavimo institucijai numatoma suteikti galimybę įgalioti asmenis, turinčius teisę įeiti į atitikties vertinimo įstaigų ir Europos kibernetinio saugumo sertifikatų turėtojų patalpas ir paimti dokumentų kopijas ir nuorašus, duomenų kopijas bei kitus daiktus, reikalingus atliekant tyrimus. Įeiti į juridinio asmens patalpas būtų galima tik juridinio asmens darbo laiku, pateikus tarnybinį pažymėjimą. Tarnybinis pažymėjimas turėtų būti suprantamas kaip bet koks pažymėjimas, patvirtinantis, kad asmuo vykdo viešojo administravimo funkcijas nacionalinėje kibernetinio saugumo sertifikavimo institucijoje ir, atsižvelgiant į tarnybos pobūdį, galėtų būti tiek valstybės tarnautojo, tiek kario pažymėjimas.

Administracinių nusižengimų kodeksą siūloma papildyti 480^1 straipsniu, skirtu administracinei atsakomybei už Kibernetinio saugumo akte nustatytos kibernetinio saugumo sertifikavimo tvarkos pažeidimus, nustatant sankcijas už:

1) Reglamente (ES) Nr. 2019/881 nustatytos informacijos apie išduotus Europos kibernetinio saugumo sertifikatus ir Europos Sąjungos atitikties pareiškimus saugojimo ar

pateikimo tvarkos pažeidimą ar viešai pateikiamos papildomos kibernetinio saugumo informacijos pateikimo ir atnaujinimo tvarkos pažeidimą. Sankcijos dydis nustatytas atsižvelgus į Administracinių nusižengimų kodekso 479 straipsnyje nustatytus sankcijų dydžius už teisės aktais nustatytų informacijos pateikimo reikalavimų pažeidimą;

2) neteisingos informacijos Europos kibernetinio saugumo sertifikatuose ir Europos Sąjungos atitikties pareiškimuose pateikimą arba Reglamente (ES) Nr. 2019/881 nustatytos informacinių ir ryšio technologijų produktų, paslaugų ir procesų, dėl kurių išduoti Europos kibernetinio saugumo sertifikatai, įvertinimo tvarkos ar Europos kibernetinio saugumo sertifikavimo schemų nuostatų pažeidimą, arba Reglamente (ES) Nr. 2019/881 nustatytos informacijos apie pažeidžiamumo spragas ar neatitikties atvejus, kurie gali daryti poveikį su sertifikavimu susijusiems reikalavimams, pateikimo tvarkos pažeidimą. Sankcijos dydis nustatytas atsižvelgus į Administracinių nusižengimų kodekso 49 straipsnio 1 dalyje ir 237 straipsnio 2 dalyje nustatytus sankcijų dydžius už ženklinimo, įteisintų produktų naudojimą pažeidžiant nustatytus reikalavimus, taip pat atsižvelgus į Administracinių nusižengimų kodekso 212 straipsnyje nustatytus sankcijų dydžius už informacijos nepateikimą ar klaidinimą bei atsižvelgus į galimo pažeidimo žalą, kadangi nacionalinėje valstybėje išduoti Europos kibernetinio saugumo sertifikatai ir Europos Sąjungos atitikties pareiškimai bus pripažįstami visoje Europos Sąjungoje.

Siūlomomis priemonėmis nustatoma atsakomybė už Kibernetinio saugumo akto III antraštinės dalies (46–65 straipsniai), 52 straipsnio 2, 4, 5, 6, 7 dalių, 53 straipsnio 2 ir 3 dalių, 54 straipsnio 1 dalies k–v punktų reikalavimų, 55 straipsnio, 56 straipsnio 4–8 dalių ir 60 straipsnio 3 ir 4 dalių pažeidimus ir taip įgyvendinamas Kibernetinio saugumo akto 65 straipsnio reikalavimas nustatyti taisykles, kuriomis reglamentuojamos už Europos kibernetinio saugumo sertifikavimo schemų nuostatų pažeidimus taikytinos veiksmingos, proporcingos ir atgrasomosios sankcijos ir imamasi visų reikiamų priemonių jų įgyvendinimui užtikrinti.

Siūloma papildyti Administracinių nusižengimų kodekso 589 straipsnio 46 dalį, nurodant, kad Nacionalinis kibernetinio saugumo centras pradeda administracinių nusižengimų teiseną, atlieka administracinių nusižengimų tyrimą, surašo administracinių nusižengimų protokolus ir naujajame 480^1 straipsnyje nurodytais atvejais. Taip Nacionaliniam kibernetinio saugumo centrui bus suteikiami Kibernetinio saugumo akto 58 straipsnio 9 dalyje numatyti įgaliojimai taikyti sankcijas, kaip numatyta Kibernetinio saugumo akto 65 straipsnyje.

Įgyvendinus siūlomus pakeitimus, bus sudarytos sąlygos tiesiogiai taikyti Kibernetinio saugumo aktą, visoje Europos Sąjungoje turėti vienodus standartus, palengvinti Europos kibernetinio saugumo sertifikatų ir Europos Sąjungos atitikties pareiškimų tarpusavio pripažinimą ir skatinti bendrą pasitikėjimą jais.

4.2. Dėl atsakingo spragų atskleidimo reglamentavimo

Siekiant įtvirtinti atsakingo spragų atskleidimo modelį, būtina numatyti, kad asmenims, atsakingai atskleidžiantiems spragas, nebūtų taikoma atsakomybė už spragų suradimą. Šiuo aspektu atkreiptinas dėmesys į tarptautinį reguliavimą, nes Lietuva yra ratifikavusi Konvenciją dėl elektroninių nusikaltimų, priimtą 2001 m. lapkričio 23 d. Budapešte, ir įgyvendinusi 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyvą 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR, kuriose numatoma pareiga nustatyti atsakomybę už neteisėtą prisijungimą prie informacinės sistemos. Baudžiamojo kodekso XXX skyriaus straipsniuose taip pat nustatomos nusikalstamos veikos sudėtys, kurių būtinasis požymis yra veikos neteisėtumas. Atsižvelgiant į tai, kad tiek nacionaliniu, tiek tarptautiniu aspektu viena iš esminių sąlygų kilti baudžiamajai atsakomybei yra atliekamų veiksmų neteisėtumas, siūloma Kibernetinio saugumo įstatyme numatyti sąlygas, kurių laikantis spragų

paieška būtų teisėta.

Kibernetinio saugumo įstatymo 2 straipsnį siūloma papildyti 12^1 dalimi, kurioje būtų pateiktas *ryšių ir informacinės sistemos spragos* sąvokos apibrėžimas.

Kibernetinio saugumo įstatymą siūloma papildyti 17 straipsniu „Spragų paieška ir atskleidimas“, kurio 1 dalyje būtų numatoma teisė asmenims ieškoti spragų, laikantis šio straipsnio 2 dalyje ir kibernetinio saugumo subjekto nustatytame spragų atskleidimo tvarkos apraše bei šio straipsnio 5 dalyje numatytų apribojimų. 2 straipsnyje siūloma numatyti tokius apribojimus:

1) negali būti trikdomas ar keičiamas ryšių ir informacinės sistemos darbas, funkcionalumas, teikiamos paslaugos bei duomenų prieinamumas ar vientisumas. Šiuo reikalavimu siekiama apsaugoti kibernetinio saugumo subjekto turtą ir duomenis nuo pakeitimų, sunaikinimo, atskleidimo ir veiklos trikdymo;

2) įsitikinus, kad spraga yra, nutraukiama spragos paieškos veikla, susijusi su rasta spraga. Šiuo reikalavimu siekiama užkirsti kelią piktnaudžiavimui rasta spraga ir nustatyti konkrečios spragos paieškos pabaigos sąlygą;

3) asmuo, vykdęs spragų paiešką, ne vėliau kaip per 24 val. nuo paieškos pradžios (paiešką tęsiant ilgiau kaip 24 val. – kas 24 val.), turi parengti nacionalinės spragų atskleidimo tvarkos apraše ar kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše nustatyto turinio informaciją apie spragų paieškos rezultatus ir ją pateikti Nacionaliniam kibernetinio saugumo centrui nacionalinės spragų atskleidimo tvarkos apraše nustatyta tvarka ir (arba) kibernetinio saugumo subjektui, kurio ryšių ir informacinėje sistemoje vykdyta paieška, šio kibernetinio saugumo subjekto nustatyta spragų atskleidimo tvarkos apraše nustatyta tvarka. Šiam reikalavimui įgyvendinti užtektų pateikti informaciją vienam iš nurodytų subjektų ir asmuo turėtų teisę pats rinktis, kam nori pateikti informaciją – kibernetinio saugumo subjektui, Nacionaliniam kibernetinio saugumo centrui ar abiem. Šiuo reikalavimu siekiama nustatyti pareigą asmeniui, vykdžiusiam spragų paiešką (net ir nenustačius spragos), pateikti informaciją apie spragų paieškos rezultatus bei nustatyti informacijos pateikimo terminą – 24 val. nuo spragos paieškos pradžios. Pažymėtina, kad atsižvelgiant į ryšių ir informacinių sistemų technologinius skirtumus bei spragų paieškos praktinį pobūdį spragų galima ieškoti neribotą laiką, tačiau susidarius situacijai, kai spragų yra ieškoma ilgiau nei 24 val., informacija apie paieškos rezultatus turėtų būti teikiama kas 24 val.;

4) nesiekiama be reikalo, daugiau, nei reikia patvirtinti spragai, stebėti, fiksuoti, perimti, įgyti, atskleisti, kopijuoti, naikinti kibernetinio saugumo subjekto valdomų ir (ar) tvarkomų duomenų. Šiuo reikalavimu siekiama apriboti prieigą prie kibernetinio saugumo subjekto duomenų iki minimumo;

5) nespėjami slaptažodžiai, nenaudojami neteisėtu būdu gauti slaptažodžiai ir nėra manipuliuojama kibernetinio saugumo subjekto darbuotojais ar kitais asmenimis, turinčiais teisę naudotis viešai neskelbtina informacija, reikšminga spragų paieškai. Šiuo reikalavimu siekiama užtikrinti, kad nebūtų užrakinamos ryšių ir informacinių sistemų paskyros, sukeliami kibernetiniai incidentai taikant automatinio veikimo priemones ir nebūtų trikdomas kibernetinio saugumo subjektų darbuotojų darbas, nebūtų galima pasinaudoti neteisėtomis priemonėmis įgyta informacija;

6) nesidalijama informacija apie rastą spragą, išskyrus šio straipsnio 2 dalies 3 punkte ir 5 dalyje nustatytais atvejais. Šiuo reikalavimu siekiama apriboti informacijos apie kibernetinio saugumo subjekto turto ir duomenų spragas perdavimą tretiesiems asmenims, iki aptikta spraga bus pašalinta.

Tik įgyvendinant visus šiuos nurodytus reikalavimus būtų galima laikyti, kad spragų ieškojimas yra teisėtas, o nesilaikant bent vieno iš šių reikalavimų būtų galima spręsti dėl baudžiamosios atsakomybės taikymo. Šis reikalavimas taikomas atsižvelgiant į tai, kad spragų ieškojimas kibernetinio saugumo subjektų ryšių ir informacinėse sistemose yra gana jautrus procesas, kurį atliekant netinkamai galima padaryti didelės žalos tiek privačių subjektų, tiek valstybės interesams, įskaitant nacionalinį saugumą. Siekiant mažinti žalos riziką, siūlomas toks

spragų paieškos teisinis reguliavimas, kad juo galėtų pasinaudoti tik specialių žinių turintys asmenys (Baudžiamojo kodekso XXX skyriaus straipsniuose nustatytų nusikalstamų veikų negalima padaryti neatsargiai). Pažymėtina, kad siūlomu pakeitimu nėra siekiama keisti Baudžiamojo kodekso XXX skyriuje nustatyto reguliavimo. Baudžiamojo kodekso XXX skyriuje uždraustos veikos ir toliau turėtų būti laikomos pavojingomis visuomenei. Atsižvelgiant į tai, kad KSĮ pakeitimo projektu nustatomos veiksmų teisėtumo sąlygos, veiksmų neteisėtumas ir toliau turėtų būti laikomas Baudžiamojo kodekso reguliavimo dalyku, todėl nėra pagrindo numatyti alternatyvos administracinės atsakomybės. Be to, siekiant mažinti žalos riziką bei atsižvelgiant į nusikalstamų veikų kibernetinėje erdvėje pobūdį, teisėsaugos institucijoms būtina palikti pakankamai veiksmingų priemonių nurodytoms nusikalstamoms veikoms tirti. Atsižvelgiant į tai, dėl neteisėto spragų ieškojimo neturėtų būti numatoma alternatyvi administracinė atsakomybė, nes tik tiriant nusikalstamas veikas būtų galima panaudoti efektyviausias informacijos rinkimo priemones.

Kibernetinio saugumo įstatymo 6 straipsnį siūloma pildyti 13 dalimi, kurioje numatoma Krašto apsaugos ministerijos kompetencija tvirtinti nacionalinės spragų atskleidimo tvarkos aprašą, o Nacionalinio kibernetinio saugumo centro kompetencija būtų nustatoma 8 straipsnio 2 dalies 16^1 punkte ir apimtų informacijos apie spragas analizę, nurodymų subjektams, valdantiems ir (ar) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjams ir elektroninės informacijos prieglobos paslaugų teikėjams dėl spragų patvirtinimo ir informavimo apie jas teikimą. Atsižvelgiant į 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 16 straipsnio 10 dalį, skaitmeninių paslaugų teikėjams papildomi saugumo ar pranešimo reikalavimai nenustatomi.

Kibernetinio saugumo įstatymo 17 straipsnio 3 dalyje siūloma nurodyti, kas turėtų būti nustatyta nacionalinės spragų atskleidimo tvarkos apraše, t. y. spragų atskleidimo tvarka, teikiamos informacijos apie spragas turinys, trumpesnių informacijos apie aptiktą spragą atskleidimo kitiems asmenims, nei nurodyta šio straipsnio 2 dalies 3 punkte, terminų nustatymo tvarka bei informacijos pateikimo Nacionaliniam kibernetinio saugumo centrui tvarka.

Kibernetinio saugumo įstatymo 17 straipsnio 4 dalyje siūloma numatyti kibernetinio saugumo subjektų teisę nustatyti savo spragų atskleidimo tvarką. Pastebėtina, kad ši teisė pati savaime nėra nauja, nes kibernetinio saugumo subjektai jau dabar turi galimybę savarankiškai nustatyti jų organizacijai taikomą atsakingo spragų atskleidimo tvarką. Įstatymo lygmeniu nustatant visiems kibernetinio saugumo subjektams taikomą bendrą spragų atskleidimo tvarką, nesiekiama kartu uždrausti kibernetinio saugumo subjektams turėti ir savo pačių nustatytos tvarkos. Siekiant, kad kibernetinio saugumo subjektai savo spragų atskleidimo tvarkos apraše nenumatytų tokių sąlygų, kurios spragų ieškojimą pernelyg apsunkintų ir iš esmės paneigtų KSĮ pakeitimo projekto tikslą, siūloma numatyti saugiklį, t. y. nuostatą, kad spragų atskleidimo tvarkos apraše numatytos spragų ieškojimo sąlygos negali būti griežtesnės, nei nurodytos 17 straipsnio 2 dalyje. Kibernetinio saugumo subjektai savo tvarkos apraše galės nustatyti tik palankesnes spragų ieškojimo sąlygas, o asmenims, nesilaikantiems kibernetinio saugumo subjektų patvirtintų griežtesnių spragų ieškojimo sąlygų, negalės būti taikoma teisinė atsakomybė, nes šios sąlygos būtų patvirtintos neteisėtai. Pažymėtina, kad kibernetinio saugumo subjektai galėtų apskritai atsisakyti spragų ieškojimo ribojimų, tačiau toks atsisakymas niekaip nepanaikintų kibernetinio saugumo subjektų atsakomybės už jų valdomas ir (arba) tvarkomas ryšių ir informacines sistemas, todėl bet koks palankesnių spragų ieškojimo sąlygų nustatymas turėtų būti atliekamas tik įvertinus galimas rizikas.

Kibernetinio saugumo įstatymo 17 straipsnio 5 dalyje siūloma numatyti galimybę spragą nustačiusiam asmeniui informaciją apie aptiktą spragą, bet ne daugiau, nei buvo pateikta Nacionaliniam kibernetinio saugumo centrui ir (ar) kibernetinio saugumo subjektui, atskleisti kitiems asmenims galiojant tam tikroms sąlygoms. Nustatoma maksimali 90 kalendorinių dienų nuo informacijos apie spragą pateikimo riba, po kurios spragą nustatęs asmuo gali informaciją atskleisti kitiems asmenims. Šios teisės suteikimas grindžiamas 2 principais: viešojo intereso ir tarpusavio kontrolės. Pirmiausia, pagal viešojo intereso principą asmuo įgauna teisę siekti visuomenei naudingų interesų, t. y. informuoti visuomenę apie nustatytas spragas ir taip paskatinti visuomenės subjektą imtis priemonių turtui ir duomenims apsaugoti, jei spragos nėra pašalinamos per nustatytą terminą. Antra, pagal tarpusavio kontrolės principą valstybės institucijos ir kibernetinio saugumo subjektai, dalyvaujantys atsakingo spragų atskleidimo procese, yra kontroliuojami visuomenės ir, gavę informaciją apie spragas, negali elgtis pasyviai. Spragų viešo atskleidimo terminas – 90 kalendorinių dienų – yra pasirinktas kaip optimalus laikotarpis, per kurį gali būti pašalinta spraga arba surasti jos valdymo būdai.

Pritarus siūlomam atsakingo spragų atskleidimo modeliui, atsiras teisinis aiškumas dėl asmenų, aptikusių spragas, teisinės padėties, bus sudarytos sąlygos teisėtai pranešti apie spragas, koordinuoto proceso metu šias spragas pašalinti ir pagerinti kibernetinio saugumo situaciją Lietuvoje.

4.3. Dėl techninių kibernetinio saugumo priemonių

Kibernetinio saugumo įstatymo 6 straipsnio 9 dalį siūloma papildyti nauja Krašto apsaugos ministerijos funkcija – tvirtinti techninių kibernetinio saugumo priemonių sąrašą, kuriame nurodoma kibernetinio saugumo priemonių paskirtis ir tvarkomi duomenys (jei jie yra tvarkomi). Taip bus aprašomos techninės kibernetinio saugumo priemonės ir kibernetinio saugumo subjektai turės aiškesnį suvokimą, kokio pobūdžio priemonės yra diegiamos jų valdomose ryšių ir informacinėse sistemose.

Priėmus siūlomus pakeitimus dėl techninių kibernetinio saugumo priemonių, bus aiškesnis teisinis reguliavimas, nustatomos techninių kibernetinio saugumo priemonių naudojimo ribos ir didinamas pasitikėjimas tarp kibernetinio saugumo subjektų ir Nacionalinio kibernetinio saugumo centro.

4.4. Dėl Kibernetinio saugumo informacinio tinklo

Kibernetinio saugumo įstatymo 13 straipsnio 1 dalyje siūloma nustatyti, kad Kibernetinio saugumo informacinis tinklas yra valstybės informacinė sistema, kurios paskirtis – informacinių technologijų priemonėmis tvarkyti duomenis, surinktus techninėmis kibernetinio saugumo priemonėmis, siekiant užkardyti ir valdyti kibernetinius incidentus, keistis informacija apie galimus ir įvykusius kibernetinius incidentus straipsnio naujoje 4 dalyje nustatytais atvejais, taip pat kita, su kibernetinio saugumo užtikrinimu susijusia, informacija. Taip bus nustatoma sąsaja tarp techninių kibernetinio saugumo priemonių ir Kibernetinio saugumo informacinio tinklo, nurodant, kad Kibernetinio saugumo informaciniame tinkle yra tvarkomi techninėmis kibernetinio saugumo priemonėmis surinkti duomenys. Taip pat nustatoma, kad Kibernetinio saugumo informacinis tinklas yra informacinė sistema, vykdanti duomenų apdorojimo ir saugojimo funkciją, tuo tarpu Kibernetinio saugumo informacinis tinklas organizaciniu požiūriu turėtų būti suvokiamas kaip specialiosios srities duomenų arba pranešimų perdavimo ir apdorojimo sistema, jungianti įvairias įstaigas.

KSĮ pakeitimo projekto 4 dalyje siūloma nustatyti, kad Kibernetinio saugumo informacinio tinklo duomenys, susiję su kibernetiniais incidentais, yra konfidencialūs, ir nurodyti atvejus, kada šie duomenys galėtų būti teikiami:

1) Kibernetinio saugumo informacinio tinklo nariams tiek, kiek tai susiję su jų valdomomis ir (arba) tvarkomomis ryšių ir informacinėmis sistemomis. Šis atvejis siejamas su tuo, kad kibernetinio saugumo subjektai turėtų galimybę gauti informaciją apie jų valdomose ir (ar) tvarkomose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus;

2) Nacionaliniam kibernetinio saugumo centrui vykdant šios įstatymo 8 straipsnio 2 dalies 13 punkte nustatytą funkciją. Šis atvejis siejamas su tuo, kad Nacionalinis kibernetinio saugumo centras, pasikonsultavęs su kibernetinio saugumo subjektu, siekdamas išvengti kibernetinio incidento arba valdyti vykstantį kibernetinį incidentą, galėtų vykdyti visuomenės informavimo funkciją;

3) jeigu galimybė teikti šiuos duomenis yra nustatyta įstatymuose ar jų pagrindu priimtuose teisės aktuose.

Priėmus siūlomus pakeitimus, bus aiškesnis teisinis Kibernetinio saugumo informacinio tinklo reguliavimas ir užtikrinamas Kibernetinio saugumo informaciniame tinkle saugomų duomenų saugumas.

5. Numatomo teisinio reguliavimo poveikio vertinimo rezultatai (jeigu rengiant įstatymų projektus toks vertinimas turi būti atliktas ir jo rezultatai nepateikiami atskiru dokumentu), galimos neigiamos priimtų įstatymų pasekmės ir kokių priemonių reikėtų imtis, kad tokių pasekmių būtų išvengta

Numatomo teisinio reguliavimo poveikio vertinimas atliekamas tik dėl Kibernetinio saugumo įstatymo pakeitimo, susijusio su atsakingo spragų atskleidimo reglamentavimu, pažyma pridedama.

Numatoma, kad įstatymų projektai neturės neigiamų pasekmių.

6. Kokią įtaką priimti įstatymai turės kriminogeninei situacijai, korupcijai

Įstatymų projektai neturės įtakos kriminogeninei situacijai ir korupcijai.

7. Kaip įstatymų įgyvendinimas atsilieps verslo sąlygoms ir jo plėtrai

Įstatymų įgyvendinimas turės įtakos kuriant saugesnę kibernetinę erdvę Lietuvos Respublikoje, todėl turėtų didinti informacinių technologijų paslaugų, procesų ir produktų patikimumą, sudaryti sąlygas verslui viešinti informaciją apie jų sukurtų informacinių technologijų paslaugų, procesų ir produktų patikimumą ir saugumą bei sudaryti sąlygas verslo, teikiančio informacinių technologijų paslaugų, procesų ir produktų atitikties Europos Komisijos patvirtintoms schemoms vertinimus, plėtrai.

8. Įstatymo projekto atitiktis strateginio lygmens planavimo dokumentams

Įstatymų projektais įgyvendinamos Kibernetinio saugumo akto III antraštinės dalies ir Kibernetinio saugumo strategijos 38.3 papunktyje nurodyto uždavinio nuostatos, Įstatymų projektai neprieštarauja strateginio lygmens planavimo dokumentams.

9. Įstatymų pakeitimo projektų inkorporavimas į teisinę sistemą, kokius teisės aktus būtina priimti, kokius galiojančius teisės aktus reikia pakeisti ar pripažinti netekusiais galios

Kartu su KSĮ pakeitimo projektu teikiamas ir ANK pakeitimo projektas.

10. Ar įstatymų projektai parengti laikantis Lietuvos Respublikos valstybinės kalbos, Teisėkūros pagrindų įstatymų reikalavimų, o įstatymų projektų sąvokos ir jas įvardijantys terminai įvertinti Terminų banko įstatymo ir jo įgyvendinamųjų teisės aktų nustatyta tvarka

Įstatymų projektai parengti laikantis Lietuvos Respublikos valstybinės kalbos įstatymo, Lietuvos Respublikos teisėkūros pagrindų įstatymo reikalavimų. KSĮ pakeitimo projektu siūlomas terminas aprobuotas Lietuvos Respublikos terminų banko įstatymo nustatyta tvarka.

11. Ar įstatymų projektai atitinka Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos nuostatas ir Europos Sąjungos dokumentus

Įstatymų projektai atitinka Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos nuostatas ir Europos Sąjungos dokumentus.

12. Jeigu įstatymui įgyvendinti reikia įgyvendinamųjų teisės aktų, – kas ir kada juos turėtų priimti

Krašto apsaugos ministras iki 2021 m. birželio 27 d. turės patvirtinti šiuos teisės aktus:

1) Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2017 m. rugpjūčio 31 d. įsakymu Nr. V-804 „Dėl Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatų ir struktūros patvirtinimo“, pakeitimo projektą;

2) Kibernetinio saugumo informacinio tinklo nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2019 m. lapkričio 27 d. įsakymu Nr. V-998 „Dėl Kibernetinio saugumo informacinio tinklo nuostatų patvirtinimo“, pakeitimo projektą;

3) krašto apsaugos ministro įsakymą dėl nacionalinės spragų atskleidimo tvarkos aprašo patvirtinimo;

4) krašto apsaugos ministro įsakymą dėl techninių kibernetinio saugumo priemonių sąrašo patvirtinimo.

Nacionalinis kibernetinio saugumo centras iki 2021 m. birželio 27 d. turės patvirtinti tyrimų dėl Reglamento (ES) 2019/881 galimo pažeidimo atlikimo tvarkos aprašą, atitikties vertinimo įstaigų įvertinimo kibernetinio saugumo sertifikavimo srityje tvarkos aprašą bei įgaliojimų atitikties vertinimo įstaigoms pagal Reglamento (ES) 2019/881 60 straipsnio 3 dalį suteikimo, apribojimo, sustabdymo arba atšaukimo tvarkos aprašą.

13. Kiek valstybės, savivaldybių biudžetų ir kitų valstybės įsteigtų fondų lėšų prireiks įstatymams įgyvendinti, ar bus galima sutaupyti (pateikiami prognozuojami rodikliai einamaisiais ir artimiausiais 3 biudžetiniais metais)

Papildomų valstybės biudžeto lėšų reikės įgyvendinant KSĮ pakeitimo projektą, nes pagal Kibernetinio saugumo aktą naujai priskirtoms funkcijoms vykdyti reikės papildomų žmogiškųjų ir finansinių išteklių. Atitinkamai Kibernetinio saugumo akto 58 straipsnio 5 punktas nustato, kad valstybės narės turi užtikrinti, kad nacionalinės kibernetinio saugumo sertifikavimo institucijos turėtų pakankamai išteklių savo įgaliojimams ir pavestoms užduotims veiksmingai bei efektyviai vykdyti. Atlikus galimybių studiją dėl Lietuvos rinkos subjektų poreikio ir gebėjimų dalyvauti kibernetinio saugumo sertifikavimo sistemoje bei nacionalinei kibernetinio saugumo sertifikavimo institucijai reikalingų gebėjimų ir jų įgijimo sertifikavimo funkcijoms atlikti, identifikuota, kad siekiant užtikrinti Reglamente (ES) 2019/881 nustatytų nacionalinės kibernetinio saugumo sertifikavimo institucijos priežiūros funkcijų vykdymą reikalingas šis finansavimas: nuo 2022 m. po 200 tūkst. Eur kasmet. Reglamente (ES) 2019/881 nustatytų nacionalinės kibernetinio saugumo

sertifikavimo institucijos sertifikavimo funkcijų vykdymo poreikis gali vystytis pagal skirtingus scenarijus, tačiau labiausiai tikėtina, kad trumpuoju laikotarpiu (1–2 metus) jis išliks nežymus, todėl šiai funkcijai vykdyti lėšų poreikio šiuo metu nėra.

14. Įstatymų projektų rengimo metu gauti specialistų vertinimai ir išvados

Įstatymų projektų rengimo metu specialistų vertinimų ir išvadų negauta.

15. Reikšminiai žodžiai, kurių reikia šiems projektams įtraukti į kompiuterinę paieškos sistemą, įskaitant Europos žodyno „Eurovoc“ terminus, temas bei sritis

„Kibernetinis saugumas“, „Kibernetinio saugumo aktas“, „sertifikavimas“, „nacionalinė kibernetinio saugumo sertifikavimo institucija“, „kibernetinio saugumo sertifikavimo sistema“, „ryšių ir informacinių sistemų spraga“, „ryšių ir informacinių sistemų spragų atskleidimas“.

16. Kiti, iniciatorių nuomone, reikalingi pagrindimai ir paaiškinimai

Nėra.

_____