LIETUVOS RESPUBLIKOS

KIBERNETINIO SAUGUMO ĮSTATYMO NR. XII-1428, LIETUVOS RESPUBLIKOS AVIACIJOS ĮSTATYMO NR. VIII-2066 41 STRAIPSNIO PAKEITIMO, LIETUVOS RESPUBLIKOS ADMINISTRACINIŲ NUSIŽENGIMŲ KODEKSO 479, 480 IR 589 STRAIPSNIŲ BEI PRIEDO PAKEITIMO, LIETUVOS RESPUBLIKOS ELEKTRONINIŲ RYŠIŲ ĮSTATYMO NR. IX-2135 3, 8, 36, 45, 51, 74, 82 IR 98 STRAIPSNIŲ PAKEITIMO, LIETUVOS RESPUBLIKOS NACIONALINIAM SAUGUMUI UŽTIKRINTI SVARBIŲ OBJEKTŲ APSAUGOS ĮSTATYMO NR. IX-1132 1, 2, 13 IR 18 STRAIPSNIŲ PAKEITIMO, LIETUVOS RESPUBLIKOS ELEKTRONINĖS ATPAŽINTIES IR ELEKTRONINIŲ OPERACIJŲ PATIKIMUMO UŽTIKRINIMO PASLAUGŲ ĮSTATYMO NR. XIII-1120 4 STRAIPSNIO PAKEITIMO, LIETUVOS RESPUBLIKOS VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ VALDYMO ĮSTATYMO NR. XI-1807 1, 3, 7, 14, 15, 26, 27, 39, 41, 42 ir 43 STRAIPSNIŲ PAKEITIMO, LIETUVOS RESPUBLIKOS VIEŠŲJŲ PIRKIMŲ ĮSTATYMO NR. I-1491 2, 17, 37, 47 ir 87 STRAIPSNIŲ PAKEITIMO, LIETUVOS RESPUBLIKOS PIRKIMŲ, ATLIEKAMŲ VANDENTVARKOS, ENERGETIKOS, TRANSPORTO AR PAŠTO PASLAUGŲ SRITIES PERKANČIŲJŲ SUBJEKTŲ, ĮSTATYMO NR. XIII-328 2, 29, 50 ir 95 STRAIPSNIŲ PAKEITIMO, LIETUVOS RESPUBLIKOS VALSTYBĖS IR TARNYBOS PASLAPČIŲ ĮSTATYMO NR. VIII-1443 4 IR 7 STRAIPSNIŲ PAKEITIMO ĮSTATYMŲ PROJEKTŲ

AIŠKINAMASIS RAŠTAS

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

Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo projektas (toliau – KSĮ projektas) parengtas siekiant įgyvendinti 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyvą (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (toliau – TIS 2 direktyva), ir 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas (toliau – Reglamentas).

TIS 2 direktyva nustato priemones, kuriomis siekiama užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Europos Sąjungoje (toliau – ES), kad būtų pagerintas vidaus rinkos veikimas, o įgyvendinant šį tikslą, TIS 2 direktyva:

1) valstybėms narėms nustatoma pareiga priimti nacionalinę kibernetinio saugumo strategiją;

2) nustatomos valstybių narių pareigos paskirti nacionalines kompetentingas institucijas, kibernetinių krizių valdymo institucijas, bendrąjį kibernetinio saugumo kontaktinį punktą ir reagavimo į kompiuterių saugumo incidentus tarnybas;

3) apibrėžiamos kibernetinio saugumo rizikos valdymo priemonės ir pareigos pranešti apie kibernetinius incidentus esminiams ir svarbiems subjektams, taip pat subjektams, identifikuotiems kaip ypatingos svarbos subjektai pagal Direktyvą (ES) 2022/2557;

4) nustatomos valstybių narių pareigos priežiūros ir vykdymo užtikrinimo srityse, taip pat pareigos keistis kibernetinio saugumo informacija.

TIS 2 direktyva įpareigoja valstybes nares priimti ir paskelbti su šios direktyvos laikymusi susijusias nacionalinės teisės nuostatas iki 2024 m. spalio 17 d. Reglamentu įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas. Jame nustatomos nacionalinių koordinavimo centrų skyrimo ir Kibernetinio saugumo kompetencijos bendruomenės įsteigimo taisyklės. Kompetencijos centrui tenka esminis vaidmuo įgyvendinant Skaitmeninės Europos programos kibernetinio saugumo elementus.

KSĮ projekto tikslas – įgyvendinti TIS 2 direktyvą ir Reglamentą Lietuvos Respublikoje, kad būtų užtikrinta nacionalinių teisės aktų atitiktis TIS 2 direktyvai ir Reglamentui, o įgyvendinant šį tikslą, nustatomi šie KSĮ projekto uždaviniai:

1) patikslinti institucijų, atsakingų už kibernetinio saugumo politikos formavimą ir įgyvendinimą, funkcijas, taip pat nustatyti kibernetinio saugumo subjektų identifikavimo kriterijus bei registravimo tvarką;

2) apibrėžti kibernetinio saugumo rizikos valdymo priemones ir pareigas kibernetinio saugumo subjektams pranešti apie kibernetinius incidentus;

3) nustatyti asmenų, atsakingų už kibernetinį saugumą, pareigas;

4) nustatyti priežiūros ir vykdymo užtikrinimo priemones ir pareigas;

5) nustatyti Kibernetinio saugumo kompetencijos bendruomenės registravimo, išregistravimo ir sprendimo apskundimo tvarką.

Įgyvendinant išdėstytus uždavinius, KSĮ dėstomas nauja redakcija, o siekiant siūlomo teisinio reguliavimo suderinamumo, kartu su KSĮ projektu teikiami kiti įstatymų projektai (toliau kartu – Įstatymų projektai), susiję su ypatingos svarbos informacinės infrastruktūros sąvokos keitimu, informacinių išteklių saugos konsolidavimu, administracinių baudų nustatymu KSĮ projekte, taip pat atsižvelgiant į TIS 2 direktyvos 42 ir 43 straipsnius, kuriais panaikinami kitų ES teisės aktų straipsniai (Reglamento (ES) Nr. 910/2014 19 straipsnis ir Direktyvos (ES) 2018/1972 40 ir 41 straipsniai išbraukiami nuo 2024 m. spalio 18 d.):

1. Lietuvos Respublikos aviacijos įstatymo Nr. VIII-2066 41 straipsnio pakeitimo įstatymo projektas;

2. Lietuvos Respublikos administracinių nusižengimų kodekso 479, 480 ir 589 straipsnių bei priedo pakeitimo įstatymo projektas (toliau – ANK projektas);

3. Lietuvos Respublikos elektroninių ryšių įstatymo Nr. IX-2135 3, 8, 36, 45, 51, 74, 82 ir 98 straipsnių pakeitimo įstatymo projektas;

4. Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo Nr. IX-1132 1, 2, 13 ir 18 straipsnių pakeitimo įstatymo projektas;

5. Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo Nr. XIII-1120 4 straipsnio pakeitimo įstatymo projektas;

6. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 1, 3, 7, 14, 15, 26, 27, 39, 41, 42 ir 43 straipsnių pakeitimo įstatymo projektas;

7. Lietuvos Respublikos viešųjų pirkimų įstatymo Nr. I-1491 2, 17, 37, 47 ir 87 straipsnių pakeitimo įstatymo projektas;

8. Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymo Nr. XIII-328 29, 50 ir 95 straipsnių pakeitimo įstatymo projektas;

9. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo Nr. VIII-1443 4 ir 7 straipsnių pakeitimo įstatymo projektas.

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

Įstatymų projektus rengė Lietuvos Respublikos krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų politikos grupės (grupės vadovė Inga Sūnelaitienė, tel. +370 706 80 800, el. p. inga.sunelaitiene@kam.lt) patarėjas mjr. Miroslavas Tribockis (tel. +370 706 80 813, el. p. miroslavas.tribockis@kam.lt), patarėja Sigita Laurinčiukaitė (tel. +370 706 80 804, el. p. sigita.laurinciukaite@kam.lt), vyresn. patarėja Aušra Pipirienė (tel. +370 706 80 808, el. p. ausra.pipiriene@kam.lt) ir Krašto apsaugos ministerijos Teisės departamento (direktorė Judita Nagienė, tel. +370 706 80 545, el. p. judita.nagiene@kam.lt) Teisėkūros skyriaus (vedėjas Tomas Vainius, tel. +370 706 80 563, el. p. tomas.vainius@kam.lt) patarėjas mjr. Mantas Keliotis (tel. +370 706 80 597, el. p. mantas.keliotis@kam.lt).

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

Galiojančiu KSĮ yra įgyvendinama Direktyva (ES) 2016/1148, kuri keičiama TIS 2 direktyva. Atsižvelgiant į Direktyvoje (ES) 2016/1148 nustatytus reikalavimus, galiojančiame KSĮ:

1. Nustatytas įpareigojimas Lietuvos Respublikos Vyriausybei nustatyti kibernetinio saugumo politikos strateginius tikslus ir (arba) pažangos uždavinius tvirtinant Nacionalinį pažangos planą (KSĮ 5 straipsnio 1 punktas).

2. Nustatytas įpareigojimas Vyriausybei tvirtinti ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką ir ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą (KSĮ 5 straipsnio 3 punktas). Pažymėtina, kad TIS 2 direktyva nustatomas kur kas platesnis subjektų, kuriems turėtų būti taikomas reguliavimas, spektras, todėl ypatingos svarbos informacinės infrastruktūros identifikavimo procesas ir identifikavimo kriterijai neatitinka TIS 2 direktyvos subjektų identifikavimo kriterijų ir tikslų, kuriais vadovaujantis būtų nustatytos dvi subjektų grupės – esminių ir svarbių subjektų.

3. Nustatytos diferencijuotos subjektų, kuriems taikomi KSĮ reikalavimai (kibernetinio saugumo subjektų), pareigos atsižvelgiant į kibernetinio saugumo subjekto tipą, įskaitant pareigą įgyvendinti Vyriausybės tvirtinamus organizacinius ir techninius kibernetinio saugumo reikalavimus ir pareigą pranešti apie kibernetinius incidentus Nacionalinio kibernetinio saugumo incidento valdymo plano, tvirtinamo Vyriausybės, nustatyta tvarka (KSĮ 11 ir 12 straipsniai). Už šių pareigų nevykdymą numatoma atsakomybė Lietuvos Respublikos administracinių nusižengimo kodekso 479 ir 480 straipsniuose. Pažymėtina, kad TIS 2 direktyva nustato išsamesnius tiek kibernetinio saugumo rizikos valdymo, tiek pranešimo apie incidentus valdymo reikalavimus, be to, skirtingai nuo Direktyvos (ES) 2016/1148, nustato ir konkrečius įpareigojamus tiriant TIS 2 direktyvos reikalavimų pažeidimus, taip pat numato ir atsakomybę už pažeidimus. Galiojantis KSĮ reguliavimas neatspindi šių TIS 2 direktyvos nuostatų.

4. Nacionaliniam kibernetinio saugumo centrui (toliau – NKSC) suteikti įgaliojimai veikti kaip nacionalinei tinklų ir informacinių sistemų saugumo kompetentingai institucijai, bendrajam informaciniam centrui ir reagavimo į kompiuterinius saugumo incidentus tarnybai (KSĮ 8 straipsnis). Pažymėtina, kad TIS 2 direktyvoje išplečiami šių institucijų įgaliojimai, ypač dėl TIS 2 direktyvos reikalavimų pažeidimų tyrimo, kurie neatsispindi galiojančiame KSĮ.

Galiojančiame KSĮ taip pat nustatomas ir nacionalinis kibernetinio saugumo teisinis reguliavimas:

1. Nustatomas kibernetinio saugumo politikos formavimo ir įgyvendinimo modelis – politiką formuojančios ir įgyvendinančios institucijos (Vyriausybė, Krašto apsaugos ministerija, Kibernetinio saugumo taryba, NKSC, Valstybinė duomenų apsaugos inspekcija, policija) ir jų funkcijos (KSĮ 4–10 straipsniai). Šioms institucijoms siūlymus teikia patariamoji institucija – Kibernetinio saugumo taryba (KSĮ 7 straipsnis), tačiau praktikoje pastebėta, kad kai kurios Kibernetinio saugumo tarybos funkcijos dubliuojasi su NKSC veikla (kibernetinio saugumo užtikrinimo būklės analizė, siūlymų teikimas kitoms institucijoms ar kibernetinio saugumo subjektams), todėl Kibernetinio saugumo tarybos funkcijos turėtų būti tikslinamos, atitinkamai keičiant ir kitus susijusius aspektus (Kibernetinio saugumo tarybos sudarymo principus).

2. Subjektų, kuriems taikomi KSĮ reikalavimai (kibernetinio saugumo subjektai), grupė galiojančiame KSĮ yra didesnė nei subjektų, kuriems taikoma Direktyva (ES) 2016/1148, grupė. Be ypatingos svarbos informacinės infrastruktūros valdytojų (pagal Direktyvą (ES) 2016/1148 suprantamų kaip esminių paslaugų operatoriai) ir skaitmeninių paslaugų teikėjų, galiojančiame KSĮ kibernetinio saugumo subjektais taip pat laikomi ir subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų teikėjai (KSĮ 2 straipsnio 8 dalis). Pažymėtina, kad kibernetinio saugumo subjektais nelaikomi aukščiausio lygio domenų vardų registravimo ir domenų vardų registravimo paslaugas teikiantys subjektai, kuriems TIS 2 direktyvoje nustatomi išskirtiniai reikalavimai. Taip pat KSĮ 1 straipsnio 2 dalyje nustatyta, kad KSĮ netaikomas patikimumo užtikrinimo paslaugų teikėjams, tačiau, vadovaujantis TIS 2 direktyva, patikimumo užtikrinimo paslaugų teikėjai, kuriems taikomas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014, turėtų būti įtraukti į TIS 2 direktyvos taikymo sritį, kad būtų užtikrintas toks pat saugumo reikalavimų

ir priežiūros lygis, koks anksčiau Reglamente Nr. 910/2014 buvo nustatytas patikimumo užtikrinimo paslaugų teikėjams.

3. Nustatomas Kibernetinio saugumo informacinis tinklas (toliau – KSIT), kurio pagrindinė 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, taip pat kita su kibernetinio saugumo užtikrinimu susijusia informacija. Atkreiptinas dėmesys, kad 2024 m. gegužės 1 d. įsigalioja papildomos KSĮ nuostatos, susijusios su KSIT naudojimu teikiant privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę, tačiau šie pakeitimai nesusiję su TIS 2 direktyvos įgyvendinimu.

4. Nustatomas ryšių ir informacinių sistemų spragų atskleidimo modelis (KSĮ 17 straipsnis) – nustatomas spragų paieškos ir atskleidimo procesas, apribojimai, kurių turi būti laikomasi atliekant spragų paiešką. Pažymėtina, kad TIS 2 direktyvoje nustatomi papildomi reikalavimai ir sąlygos, susijusios su spragų atskleidimo procesu, tačiau tai nesukuria pagrindo iš esmės keisti spragų paieškos ir atskleidimo proceso ir apribojimų.

5. Nustatomos valstybės informacinių išteklių saugos nuostatos. Subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, galiojančio KSĮ VII skyriuje yra numatytos išskirtinės pareigos, susijusios su valstybės informacinių išteklių sauga. Pažymėtina, kad TIS 2 direktyvos reikalavimai turi būti taikomi ir viešojo administravimo subjektams, kurie laikomi esminiais subjektais, todėl šios galiojančios valstybės informacinių išteklių saugos nuostatos atitinkamai turi būti tikslinamos pagal TIS 2 direktyvos reikalavimus. KSĮ 22 straipsnyje apibrėžtos saugos įgaliotinio funkcijos, kuris atsako už saugos reikalavimų vykdymą ir atlieka informacinės sistemos saugos nuostatuose ir kituose valstybės informacinių išteklių saugą reglamentuojančiuose teisės aktuose nustatytas funkcijas, o KSĮ 11 straipsnio 1 dalies 5 punkte nustatyta, kad kibernetinio saugumo subjektai paskiria kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir NKSC pateikia šio asmens ar padalinio kontaktinę informaciją, tačiau nėra apibrėžtos kompetentingo asmens ar padalinio funkcijos ir pareigos. Išanalizavus KSĮ 22 straipsnio ir 11 straipsnio 1 dalies 5 punkto nuostatas darytina išvada, kad nėra aiškios atskirties tarp šių nurodytų pareigybių.

6. Sudarant sąlygas taikyti Reglamentą (ES) 2019/881, galiojančio KSĮ VI skyriuje nustatomi nacionalinės kibernetinio saugumo sertifikavimo institucijos įgaliojimai. Šiame skyriuje nustatytos nuostatos yra pakankamos Reglamentui (ES) 2019/881 taikyti, KSĮ projektu jų keisti neketinama.

7. Krašto apsaugos ministerija, vadovaudamasi Lietuvos Respublikos Vyriausybės 1998 m. liepos 23 d. nutarimu Nr. 924 „Dėl Lietuvos Respublikos krašto apsaugos ministerijos nuostatų patvirtinimo“, vykdo Reglamento 7 straipsnyje nustatytas Nacionalinio koordinavimo centro (toliau – NKC) užduotis, tačiau KSĮ nėra nustatytos Kibernetinio saugumo kompetencijos bendruomenės, jos registravimo, išregistravimo, sprendimo apskundimo nuostatos, kaip to reikalaujama Reglamente.

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

Perkeliant TIS 2 direktyvą KSĮ projekte atlikti tokie pakeitimai:

1. Priėmus TIS 2 direktyvą, kartu keičiami ir kiti ES teisės aktai – iš Reglamento (ES) Nr. 910/2014 išbraukiamas 19 straipsnis, kadangi patikimumo užtikrinimo paslaugų teikėjai, kuriems taikomas Reglamentas (ES) Nr. 910/2014, įtraukti į TIS 2 direktyvos taikymo sritį.

2. TIS 2 direktyvos 4 straipsnyje numatoma, kad jeigu tam tikruose sektoriuose veikiantiems esminiams ir svarbiems subjektams pagal konkretiems sektoriams taikomus ES teisės aktus numatomos priežiūros ir vykdymo užtikrinimo priemonės yra lygiavertės TIS 2 direktyvoje numatytoms priemonėms, šiems subjektams netaikomos TIS 2 direktyvos nuostatos, susijusios su priežiūra ir vykdymo užtikrinimu. Atsižvelgiant į tai, KSĮ projekto 1 straipsnio 3 dalyje siūloma numatyti tam tikrų įstatymo nuostatų (susijusių su kibernetinio saugumo rizikos valdymo priemonių įgyvendinimu, pranešimu apie didelius kibernetinius incidentus) netaikymo išimtis tais atvejais, jei konkrečiam sektoriui taikomame ES teisės akte yra lygiavertį poveikį turinčios nuostatos. Kriterijai,

kuriais vadovaujantis nustatomas nuostatų lygiavertiškumas, numatomi KSĮ projekto 1 straipsnio 4 dalyje. Šie kriterijai atitinka TIS 2 direktyvos 4 straipsnio 2 dalyje numatomus lygiavertiškumo vertinimo kriterijus, juos papildžius pagal 2023 m. rugsėjo 13 d. Europos Komisijos gairėse dėl TIS 2 direktyvos 4 straipsnio 1 ir 2 dalių taikymo pateiktą išaiškinimą dėl TIS 2 direktyvos 4 straipsnio 1 ir 2 dalių taikymo. Be to, atsižvelgiant į Reglamento (ES) 2022/2554 5 straipsnio 3 dalį, nustatomos analogiškos išimtys iš reikalavimų skirti už kibernetinį saugumą atsakingus asmenis. Atsižvelgiant į tai, kad TIS 2 direktyvos 4 straipsnio 2 dalyje nurodyti lygiavertiškumo vertinimo kriterijai yra vertinamojo pobūdžio, ir siekiant nesukurti situacijos, kai kaskart ES priėmus naują konkrečiam sektoriui taikomą ES teisės aktą būtų keičiamas KSĮ dėl išimties nustatymo, KSĮ projektu siūloma numatyti, kad lygiavertį poveikį turinčių konkrečiam sektoriui taikomų ES teisės aktų sąrašą patvirtintų Vyriausybė nutarimu (KSĮ projekto 1 straipsnio 5 dalis). Siūloma numatyti, kad nurodytas Vyriausybės nutarimas būtų tvirtinamas atskiruose sektoriuose politiką formuojančių ministerijų teikimu, atsižvelgiant į tai, kad konkretiems sektoriams taikomus ES teisės aktus pagal kompetenciją geriausiai išmano šiuose sektoriuose politiką formuojančios institucijos.

TIS 2 direktyvos 2 straipsnyje numatoma TIS 2 direktyvos netaikymo išimtis subjektams, vykdantiems veiklą nacionalinio saugumo, visuomenės saugumo, gynybos ar teisėsaugos srityse, todėl siūloma KSĮ netaikyti žvalgybos tarnyboms įvertinus Lietuvos Respublikos žvalgybos įstatymo nuostatas. Atsižvelgiant į besiformuojančią praktiką įgyvendinant Reglamento (ES) 2022/2554 2 straipsnio 4 dalyje valstybėms narėms nustatytą pasirinkimo galimybę netaikyti Reglamento (ES) 2022/2554 nuostatų Direktyvos 2013/36/ES 2 straipsnio 5 dalies 4–23 punktuose nurodytiems subjektams, esantiems jų atitinkamose teritorijose (Lietuvoje tokie subjektai yra kredito unijos), nustatomos dalinės išimtys centrinėmis kredito unijomis nelaikomoms kredito unijoms.

3. Į nacionalinę teisę perkeliant TIS 2 direktyvos 6 straipsnyje pateiktas sąvokas atsižvelgta į tai, kad TIS 2 direktyvoje pateikiamos sąvokos yra glaudžiai susijusios su kitais ES teisės aktais (Reglamentu (ES) 2019/881, Reglamentu (ES) Nr. 1025/2012, Reglamentu (ES) Nr. 910/2014, Reglamentu (ES) 2019/1150), todėl pasirinkta šiuose teisės aktuose apibrėžtų sąvokų, kiek įmanoma, iš naujo neapibrėžti, o vartoti jau kituose teisės aktuose apibrėžtas sąvokas. Atkreiptinas dėmesys, kad nors TIS 2 direktyvoje pateikiamose sąvokose yra nemažai techninio pobūdžio formuluočių (aukščiausio lygio domenas, kintamo masto pritaikoma bendrų ir paskirstytų kompiuterijos išteklių bazė, interneto maršruto parinkimo ir junglumo paslaugos, rekursinio domenų vardų keitimo paslaugos, šakninių vardų serveriai), šios formuluotės vartojamos ir kituose ES teisės aktuose jų neapibrėžiant, todėl siekiant neiškreipti kituose ES teisės aktuose pateikiamų sąvokų sampratos ir atsižvelgiant į tai, kad informacinių technologijų srityje veikiantiems asmenims šios formuluotės yra aiškios ir suprantamos, šių formuluočių įstatyme siūloma neapibrėžti.

4. Nors Kibernetinio saugumo taryba nėra TIS 2 direktyvos reguliavimo sritis, tačiau, atsižvelgus į naujai atsiradusius sektorius TIS 2 direktyvoje, siūloma KSĮ projekto 6 straipsnio 2 dalyje išplėsti Kibernetinio saugumo tarybos sudėtį, kurią sudarytų politiką formuojančių, dalyvaujančių formuojant ir ją įgyvendinančių institucijų atstovai, KSĮ projekto 1 ir 2 priede nurodytų institucijų, atsakingų už kibernetinio saugumo subjektų identifikavimą, atstovai, kibernetinio saugumo subjektams atstovaujančių asociacijų, mokslo ir studijų institucijų atstovai ir šio KSĮ projekto 23 straipsnyje nurodyti Kibernetinio saugumo bendruomenės nariai. Toks pakeitimas leistų objektyviau sudaryti personalinę kibernetinio saugumo tarybos sudėtį bei įtraukti daugiau suinteresuotų subjektų atstovų.

Taip pat iš naujo įvertintos Kibernetinio saugumo tarybos funkcijos. Atsižvelgiant į veiklos praktiką, kai Kibernetinio saugumo tarybos siūlymus gauna, juos analizuoja ir jais vadovaujasi Krašto apsaugos ministerija, siūloma nustatyti, kad Kibernetinio saugumo taryba siūlymus teikia Krašto apsaugos ministerijai (KSĮ projekto 6 straipsnio 1 dalis). Atsižvelgiant į Kibernetinio saugumo tarybos kompetencijas ir žinias, nustatomos funkcijos dėl keitimosi gerąja praktika ir žiniomis kibernetinio saugumo srityje bei pasiūlymų teikimo dėl kibernetinio saugumo prioritetų, plėtros krypčių, viešojo sektoriaus, verslo ir mokslo bendradarbiavimo galimybių, kibernetinio saugumo rizikos valdymo priemonių ir kibernetinių incidentų valdymo ir kibernetinio saugumo stiprinimo krypčių.

5. NKSC funkcijos nustatomos KSĮ projekto 7 straipsnyje. KSĮ projekto 7 straipsnio 2 dalies 1–3, 6, 10, 12, 13, 16, 18, 19 punktuose išlaikomos KSĮ jau nustatytos funkcijos, 4, 5, 8, 9, 11, 14, 15 punktuose perkeltos TIS 2 direktyvoje nustatytos kompetentingų institucijų funkcijos.

KSĮ projekto 7 straipsnio 2 dalies 14 ir 15 punktuose nustatytos funkcijos, susijusios su veiksmais krizių atveju. Nors krizių atveju bus vadovaujamasi Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatymu, NKSC dalyvaus valdant krizes, susijusias su kibernetiniais incidentais, bei teiks pranešimus ES institucijoms. Tuo tarpu KSĮ projekto 8 straipsnyje siūloma nustatyti pagalbos valdant kibernetinius incidentus modelį. Šiais atvejais NKSC tvarkytų duomenis apie kibernetinio saugumo subjektus, kitas įstaigas ir ūkio subjektus, kuriems, vadovaujantis Krizių valdymo ir civilinės saugos įstatymu, būtų pavedamos būtinosios užduotys valdant kibernetinius incidentus, joms reguliariai organizuotų kibernetinio saugumo pratybas ir mokymus.

KSĮ projekto 7 straipsnio 2 dalies 15, 18 ir 19 punktuose nustatant funkcijas, susijusias su bendradarbiavimu kibernetinio saugumo srityje, be bendradarbiavimo su ES, įtraukiamos Šiaurės Atlanto sutarties organizacijos (toliau – NATO) ir kitų valstybių, taip pat ES, NATO institucijos ir tarptautinės organizacijos. Pažymėtina, kad TIS 2 direktyva kalba tik apie ES institucijas ir organizacijas, tačiau siekiant sukonstruoti bendrą sistemą siūloma nustatyti platesnio bendradarbiavimo modelį.

KSĮ projekto 7 straipsnio 2 dalies 16 ir 17 punktuose bei V skyriuje nustatytos funkcijos, apimančios atitikties kibernetinio saugumo rizikos valdymo priemonėms stebėseną, subjektų konsultavimą kibernetinio saugumo rizikos valdymo priemonių taikymo klausimais, subjektų patikrinimų vykdymą bei vykdymo užtikrinimo priemonių parinkimą ir taikymą. Pažymėtina, kad atsižvelgiant į TIS 2 direktyvos 32 straipsnio 2 dalies b punktą KSĮ projekto 7 straipsnio 3 dalyje siūloma nustatyti naują teisę NKSC pasitelkti nustatytas sąlygas atitinkantį nepriklausomą auditorių, audito įmonę ar kitą instituciją, atitinkančią NKSC nustatytus nepriklausomumo, nešališkumo ir nepriekaištingos reputacijos reikalavimus, kibernetinio saugumo auditui atlikti, kai yra vykdoma atitikties kibernetinio saugumo rizikos valdymo priemonėms stebėsena. Atliekant kibernetinio saugumo auditą turės būti užtikrinamas kibernetinio saugumo subjekto valdomų ir (ar) tvarkomų tinklų ir informacinių sistemų kibernetinis saugumas. Atkreiptinas dėmesys, kad nors Valstybės informacinių išteklių valdymo įstatymo 20 straipsnyje nustatomos valstybės informacinių išteklių valdymo audito nuostatos, kibernetinio saugumo auditas savo prasme skiriasi nuo valstybės informacinių išteklių valdymo audito, todėl šių auditų nuostatos tarpusavyje nesiejamos.

Siekiant laiku pašalinti kibernetines grėsmes ar stabdyti jų plitimą, siūloma KSĮ projekto 7 straipsnio 2 dalies 7 punkte nustatyti naują teisę NKSC duoti nurodymą viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjui ir (ar) domeno vardų paslaugų teikėjui blokuoti interneto svetainių, platinančių kenkimo kodus, apgaulės būdu renkančius prisijungimus prie tinklų ir informacinių sistemų ir (ar) naudojamus siekiant koordinuoti ir vykdyti kibernetinius incidentus, domenų vardus, taip pat kitus domenų vardus, sukurtus minėtoms interneto svetainių veikloms vykdyti.

Papildomai KSĮ 7 straipsnio 4 dalyje nustatoma teisė skųsti teismui NKSC pritaikytas priemones ir nurodymus Administracinių bylų teisenos įstatymo nustatyta tvarka. Pažymėtina, kad šio straipsnio 2 dalies 7 punkte numatoma apskundimo išimtis – nurodymus blokuoti interneto domenų vardus būtų galima skųsti Lietuvos Respublikos civilinio proceso kodekso nustatyta tvarka, atsižvelgiant į tai, kad domeno vardo blokavimas apribotų asmenų teises į jų turtą – domeno vardą.

Atsižvelgiant į TIS 2 direktyvos 11 straipsnio 1 ir 2 dalyse nustatytus reikalavimus reagavimo į kompiuterių saugumo incidentus tarnyboms (šią funkcija vykdo NKSC), KSĮ projekto 7 straipsnio 5 ir 6 dalyse nustatomi atitinkami reikalavimai.

6. Kibernetinio saugumo subjektai, kurie patenka į KSĮ projekto taikymo sritį, yra skirstomi į dvi kategorijas: esminių subjektų ir svarbių subjektų, atspindint jų svarbos mastą jų sektoriaus arba jų teikiamų paslaugų rūšies, taip pat jų dydžio požiūriais. Abiejų kategorijų subjektams taikomos priežiūros ir vykdymo užtikrinimo priemonės yra diferencijuojamos siekiant užtikrinti tinkamą rizika grindžiamų reikalavimų ir pareigų ir administracinės naštos, atsirandančios dėl atitikties priežiūros, pusiausvyrą.

Siekiant įgyvendinti TIS 2 direktyvos 3 straipsnyje nustatytus identifikavimo kriterijus ir tikslus, siūloma KSĮ projekto 11 straipsnyje nustatyti esminių ir svarbių subjektų identifikavimo kriterijus.

TIS 2 direktyvos 2 straipsnio 1 dalis nustato, kad į esminių ir svarbių subjektų kategorijas patenka viešieji ar privatieji subjektai, kurie laikomi vidutinėmis įmonėmis pagal Rekomendacijos 2003/361/EB priedo 2 straipsnį arba kurie viršija to straipsnio 1 dalyje nustatytas viršutines ribas ir kurie teikia paslaugas arba vykdo veiklą ES. Atitinkamai TIS 2 direktyvos 3 straipsnio 1 dalies a punktas ir 2 dalis nustato, kad minėtieji viešieji ar privatieji subjektai turi veikti TIS 2 direktyvos I ir II priede nurodytuose sektoriuose. Atsižvelgiant į šias nuostatas, KSĮ projekto 11 straipsnio 3 dalies 1 punkte bei 4 dalies 1 ir 2 punktuose siūloma nustatyti atitinkamus esminių kibernetinio saugumo subjektų (toliau – esminiai subjektai) ir svarbių kibernetinio saugumo subjektų (toliau – svarbūs subjektai) identifikavimo kriterijus.

TIS 2 direktyvos 3 straipsnio 1 dalies b ir c punktai nustato, kad esminiais subjektais laikomi kvalifikuoti patikimumo užtikrinimo paslaugų teikėjai ir aukščiausio lygio domenų vardų registrų teikėjai, taip pat DNS paslaugų teikėjai, nepriklausomai nuo jų dydžio, bei viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai. Atsižvelgiant į šias nuostatas, KSĮ projekto 11 straipsnio 3 dalies 2 ir 3 punktuose siūloma nustatyti atitinkamus esminių subjektų identifikavimo kriterijus. Vadovaujantis TIS 2 direktyvos 3 straipsnio 2 dalimi, nustatančia, kad subjektai, kurie nelaikomi esminiais subjektais, yra laikomi svarbiais subjektais, KSĮ projekto 11 straipsnio 4 dalies 3 ir 4 punktuose nustatyti svarbių subjektų identifikavimo kriterijai, susiję su nekvalifikuotas patikimumo užtikrinimo paslaugas teikiančių bei viešųjų elektroninių ryšių tinklų paslaugas ar viešai prieinamų elektroninių ryšių paslaugas teikiančių subjektų identifikavimu.

TIS 2 direktyvos 3 straipsnio 1 dalies d punktas nustato, kad esminiais subjektais laikomi centrinės valdžios, kaip valstybė narė apibrėžė pagal nacionalinę teisę, viešojo administravimo subjektas. Atsižvelgiant į šią nuostatą, KSĮ projekto 11 straipsnio 3 dalies 5 punkte siūloma nustatyti atitinkamą esminių subjektų identifikavimo kriterijų. Pažymėtina, kad atsižvelgiant į TIS 2 direktyvos 2 straipsnio 5 dalies a punktą, kuriuo valstybei nustatoma teisė į esminių ir svarbių subjektų kategorijas įtraukti viešojo administravimo subjektus vietos lygmeniu ir atsižvelgus į poreikį stiprinti kibernetinį saugumą sistemiškai, KSĮ projekto 11 straipsnio 3 dalies 5 punkte nustatomas esminių subjektų identifikavimo kriterijus, susijęs su regioninio administravimo subjektais ir savivaldybių administravimo subjektais pagal Viešojo administravimo įstatymą.

TIS 2 direktyvos 3 straipsnio 1 dalies f punktas nustato, kad esminiais subjektais laikomi pagal Direktyvą (ES) 2022/2557 identifikuoti ypatingos svarbos subjektai. Atsižvelgiant į šią nuostatą, KSĮ projekto 11 straipsnio 3 dalies 4 punkte siūloma nustatyti atitinkamą esminių subjektų identifikavimo kriterijų. Pažymėtina, kad subjektų pripažinimas ypatingos svarbos subjektais numatytas Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatymo Nr. VIII-971 1, 2, 7, 9, 11, 12, 13, 22, 50, 52 straipsnių ir priedo pakeitimo, įstatymo papildymo VI^{1} skyriumi ir nauju 1 priedu įstatymo projekte, pateiktame derinti Lietuvos Respublikos vidaus reikalų ministerijos.

TIS 2 direktyvos 2 straipsnio 4 dalis nustato, kad TIS 2 direktyva yra taikoma subjektams, teikiantiems domenų vardų registravimo paslaugas. Atsižvelgiant į šią nuostatą, KSĮ projekto 11 straipsnio 4 dalies 6 punkte siūloma nustatyti atitinkamą svarbių subjektų identifikavimo kriterijų.

Siekiant užtikrinti tinkamą valstybės informacinių išteklių kibernetinį saugumą, KSĮ projekto 11 straipsnio 3 dalies 6 punkte ir 4 dalies 5 punkte nustatomi esminių ir svarbių subjektų identifikavimo kriterijai, susiję su Valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka valdomais ir (ar) tvarkomais valstybės informaciniais ištekliais.

Siekiant užtikrinti tinkamą nacionaliniam saugumui užtikrinti svarbios įmonės kibernetinį saugumą, KSĮ projekto 11 straipsnio 3 dalies 7 punkte nustatomas esminių subjektų identifikavimo kriterijus, susijęs su nacionaliniam saugumui užtikrinti svarbia įmone arba asmens valdoma ir (ar) tvarkoma tinklų ir informacinė sistema.

Siekiant užtikrinti tinkamą elektroninės informacijos prieglobos paslaugas teikiančių subjektų kibernetinį saugumą, KSĮ projekto 11 straipsnio 4 dalies 7 punkte nustatomas atitinkamas svarbių subjektų identifikavimo kriterijus.

TIS 2 direktyvos 2 straipsnio 2 dalies b–e punktai nustato esminių ir svarbių subjektų identifikavimo kriterijus, kurie leidžia nacionalinei valstybei įvertinti subjekto svarbą per jo teikiamų paslaugų poveikio mastą viešajam saugumui, visuomenės saugumui, visuomenės sveikatai, sutrikimų keliamai rizikai. Šio vertinamojo pobūdžio esminių ir svarbių subjektų identifikavimo kriterijai KSĮ projekte vadinami specialiaisiais identifikavimo kriterijais ir yra nustatyti KSĮ projekto 11 straipsnio 5 dalyje. KSĮ projekto 11 straipsnio 5 dalyje 1–4 punktuose nustatyti minėtieji TIS 2 direktyvos 2 straipsnio 2 dalies b–e punktuose nustatyti identifikavimo kriterijai.

Dėl intensyvėjančių kibernetinių grėsmių ir didėjančio jų sudėtingumo siūloma nustatyti ir papildomus nacionalinius kriterijus, kurių nėra numatyta TIS 2 direktyvoje ir pagal kuriuos subjektai būtų priskiriami esminių arba svarbių subjektų grupėms, turint tikslą pasiekti aukštą kibernetinio saugumo lygį ir remti lygiaverčių kibernetinio saugumo rizikos valdymo priemonių, atspindinčių jautrų šių subjektų pobūdį, įgyvendinimą. KSĮ projekto 11 straipsnio 5 dalies 5–6 punktuose teikimo grandinių kibernetiniam saugumui stiprinti nustatyti identifikavimo kriterijai, susiję su trečiųjų šalių paslaugų teikimu viešojo administravimo sektoriui ir esminiams subjektams. KSĮ projekto 11 straipsnio 5 dalies 7 punkte, siekiant užtikrinti kibernetinį saugumą gyvybiškai svarbias valstybės funkcijas atliekantiems ir valstybinės mobilizacines užduotis vykdantiems subjektams, nustatyti atitinkami identifikavimo kriterijai. KSĮ projekto 11 straipsnio 5 dalies 8 punkte, atsižvelgiant į TIS 2 direktyvos 2 straipsnio 5 dalies b punktą, nustatytas identifikavimo kriterijus, susijęs su subjektais, mokslinių tyrimų sektoriuje vykdančiais ypatingos svarbos mokslinių tyrimų ir eksperimentinės plėtros veiklą.

Atsižvelgiant į specialiųjų identifikavimo kriterijų vertinamąjį pobūdį, siūlytina, kad Vyriausybė tvirtintų identifikavimo pagal specialiuosius kriterijus metodiką.

Mažinant subjektams tenkančią administracinę naštą pateikti esminiams ir svarbiems subjektams identifikuoti reikalingus duomenis, siekiant sudaryti palankesnes sąlygas atsakingoms institucijoms sukurti ir atnaujinti esminių ir svarbių subjektų sąrašą bei fiksuoti subjekto tapimo esminiu ir svarbiu subjektu faktą, su juo susiejant esminiam ir svarbiam subjektui atsirandančias pareigas ir pasekmes, siūloma įsteigti Kibernetinio saugumo subjektų registrą (KSĮ projekto 13 straipsnis), kuriame būtų registruojami esminiai ir svarbūs subjektai ir su subjektais susiję pagrindiniai duomenys (KSĮ projekto 13 straipsnio 3 dalis). Kibernetinio saugumo subjektų registro objektas ir jį apibūdinantys duomenys būtų tvarkomi KSIT (KSĮ projekto 13 straipsnio 2 dalis). Siūloma nustatyti, kad subjektai identifikavimo tikslams reikalingus duomenis teiktų KSIT nuostatuose nustatyta tvarka (KSĮ projekto 13 straipsnio 4 dalis), o Kibernetinio saugumo subjektus registruotų ir išregistruotų KSIT tvarkytojas (KSĮ projekto 13 straipsnio 5 dalis). Taip pat siūloma, kad esminių ir svarbių subjektų identifikavimo procese dalyvautų atsakingos institucijos, nurodytos KSĮ projekto 1 ir 2 prieduose (KSĮ projekto 13 straipsnio 6 dalis).

Siūloma nustatyti, kad KSIT tvarkytojas, KSIT nuostatuose nustatytais atvejais ir tvarka identifikuodamas ir registruodamas esminius ir svarbius subjektus, turėtų teisę neatlygintinai gauti iš identifikuojamų asmenų, kitų valstybės institucijų, valstybės įstaigų, valstybės valdomų įmonių, viešųjų įstaigų, savivaldybių įmonių ir savivaldybių įstaigų duomenis, reikalingus esminiams ir svarbiems subjektams registruoti (KSĮ projekto 13 straipsnio 7 dalis). Tuo tikslu NKSC, kaip KSIT tvarkytojas, panaudodamas atvirus duomenų šaltinius ir duomenis, gautus iš kitų duomenų šaltinių ir valstybės valdomų registrų apie asmenis (KSĮ projekto 13 straipsnio 10 dalyje nustatyta, kad sektoriai, subsektoriai ir subjekto rūšis nustatomi pagal Ekonominės veiklos rūšių klasifikatorių), bei pritaikydamas KSĮ projekte nustatytus kriterijus, sudarys esminių ir svarbių subjektų sąrašus. Subjektai atitinkamai bus informuojami elektroniniu pranešimu apie patekimą į sąrašą ir turės galimybę tikslinti duomenų tikrumą. Išsamesnis subjektų identifikavimo procesas bus nustatytas KSIT nuostatuose. Kibernetinio saugumo subjektų išregistravimo iš Kibernetinio saugumo subjektų registro sąlygos nustatytos KSĮ projekto 13 straipsnio 9 dalyje.

Subjektai turi teisę skųsti sprendimą juos registruoti Kibernetinio saugumo subjektų registre (KSĮ projekto 13 straipsnio 8 dalis).

KSIT duomenų teikimo apribojimai yra nustatyti KSĮ projekto 19 straipsnio 5 dalyje, o specialiųjų asmens duomenų tvarkymo sąlygų nustatyti neketinama.

6. TIS 2 direktyvos 21 straipsnis nustato kibernetinio saugumo valdymo priemones bei nurodo šių priemonių elementus. Nustatomos kibernetinio saugumo rizikos valdymo priemonės, grindžiamos visų rūšių pavojus apimančiu požiūriu, tarp jų ir fiziniu ir aplinkos saugumu. TIS 2 direktyvos 1 dalyje nurodoma, kad valstybės narės turi užtikrinti, kad esminiai ir svarbūs subjektai imtųsi tinkamų ir proporcingų techninių, operatyvinių ir organizacinių priemonių. Šiuo metu KSĮ taip pat nustatyta, kad kibernetinio saugumo subjektai atsako už jų valdomų ryšių ir informacinių sistemų ar teikiamų paslaugų kibernetinį saugumą, užtikrina jų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams, todėl, siekiant išlaikyti dabartinės praktikos tęstinumą ir toliau plėtoti įgytas žinias ir patirtis, siūloma KSĮ projekto 14 straipsnio 1 dalyje nustatyti, kad kibernetinio saugumo subjektai užtikrintų veiklai vykdyti ar paslaugoms teikti naudojamų tinklų ir informacinių sistemų atitiktį kibernetinio saugumo rizikos valdymo priemonėms, t. y. kibernetinio saugumo reikalavimams, tvirtinamiems Vyriausybės, ir Europos Komisijos priimtiems įgyvendinimo aktams, taikomiems konkretiems sektoriams, jei toks reguliavimas nustatytas**.**

Siūloma nustatyti, kad kibernetinio saugumo subjektai įgyvendintų kibernetinio saugumo reikalavimus per Vyriausybės nustatytą ne trumpesnį nei 12 mėn. terminą. Šį terminą Vyriausybė nustatytų tvirtindama kibernetinio saugumo reikalavimų aprašą, o šiuo terminu būtų siekiama sudaryti palankesnes sąlygas kibernetinio saugumo subjektams suplanuoti būtinus finansinius išteklius ir pajėgumus kibernetinio saugumo reikalavimams įgyvendinti (KSĮ projekto 14 straipsnio 2 dalis).

Siūloma įtvirtinti, kad kibernetinio saugumo reikalavimai apimtų elementus, kaip to reikalaujama TIS 2 direktyvos 21 straipsnio 2 dalyje. Taip pat siekiant išlaikyti dabartinės praktikos tęstinumą ir toliau plėtoti įgytas žinias ir patirtis, būtų siekiama išlaikyti šiuo metu galiojančių kibernetinio saugumo reikalavimų apimtis, į jas integruojant Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo nuostatas, taip pat papildant atskiriems sektoriams arba atskiroms kibernetinio saugumo subjektų grupėms taikomomis kibernetinio saugumo rizikos valdymo priemonėmis, kurios būtų nustatytos atsižvelgiant į atskiruose sektoriuose identifikuotas kibernetinio saugumo rizikas.

Kadangi grėsmė tinklų ir informacinių sistemų saugumui gali būti įvairios kilmės, kibernetinio saugumo reikalavimai turėtų būti grindžiami visų rūšių pavojus apimančiu požiūriu, kuriuo siekiama apsaugoti tinklų ir informacines sistemas bei jų fizinę aplinką nuo tokių įvykių kaip vagystė, gaisras, potvynis, telekomunikacijų ar elektros energijos tiekimo triktys, arba nuo neleistinos fizinės prieigos prie kibernetinio saugumo subjekto informacijos ir informacijos tvarkymo objektų ir žalos jiems, ir jų trikdžių, kurie galėtų kelti pavojų saugomų, perduodamų ar tvarkomų duomenų arba per tinklų ir informacines sistemas teikiamų ar prieinamų paslaugų prieinamumui, autentiškumui, vientisumui arba konfidencialumui, siūloma, kad kibernetinio saugumo reikalavimuose būtų detaliau aprašomos priemonės bei numatytos papildomos kibernetinio saugumo rizikos valdymo priemonės, taikomos atskiriems sektoriams arba atskiroms esminių ar svarbių subjektų grupėms, atsižvelgiant į atskiruose sektoriuose identifikuotas kibernetinio saugumo rizikas (KSĮ projekto 14 straipsnio 5 dalies 13 punktas).

Siekiant įgyvendinti TIS 2 direktyvos 20 straipsnio 2 dalį, siūloma KSĮ projekto 14 straipsnio 7 dalyje nustatyti, kad kibernetinio saugumo subjekto valdymo organų nariai, vadovas ir jo įgaliotas asmuo (taip pat galioja, jei jis yra fizinis asmuo) privalo ne rečiau kaip kartą per 2 metus NKSC vadovo nustatyta tvarka išklausyti kibernetinio saugumo mokymus bei užtikrinti kibernetinio saugumo subjekto darbuotojų nuolatinį švietimą kibernetinio saugumo srityje. Dalyvavimas mokymuose leistų įgyti pakankamai žinių ir įgūdžių nustatyti rizikas ir įvertinti kibernetinio saugumo rizikos valdymo praktiką bei jos poveikį subjekto teikiamoms paslaugoms. Pažymėtina, kad šis reikalavimas padėtų kibernetinio saugumo subjekto vadovui arba jo įgaliotam asmeniui užtikrinti KSĮ projekto 14 straipsnio 6 dalyje nustatytos pareigos – užtikrinti, kad kibernetinio saugumo subjektas laikytųsi įstatyme jam nustatytų pareigų, ir prižiūrėti jų laikymąsi – vykdymą.

KSĮ projekto 14 straipsnio 8 dalyje išlaikoma galiojančio KSĮ nuostata, kad kibernetinio saugumo subjektai ne rečiau kaip kartą per 3 metus atlieka kibernetinio saugumo auditą. Kibernetinio saugumo auditą gali atlikti nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti

informacinių sistemų auditoriai, audito įmonės ar kitos institucijos, kurios atitinka NKSC metodikoje nustatytus nepriklausomumo, nešališkumo ir nepriekaištingos reputacijos reikalavimus, ar asmenys, NKSC vadovo nustatyta tvarka išklausę mokymus ir išlaikę kvalifikacinius žinių ir praktinių įgūdžių patikrinimo egzaminą.

7. Nuostatos dėl asmenų, atsakingų už kibernetinį saugumą, įtraukiamos siekiant užtikrinti dabartinės praktikos tęstinumą ir toliau plėtoti įgytas žinias ir patirtis, taip pat siekiant, kad kibernetinio saugumo subjektai patvirtintų kibernetinio saugumo rizikos valdymo priemones ir prižiūrėtų jų įgyvendinimą subjekto veikloje. Siūloma nustatyti du už kibernetinį saugumą atsakingų asmenų lygius, skiriant kibernetinio saugumo vadovą ir saugos įgaliotinį, ir nustatyti jų pagrindines pareigas.

Siūloma nustatyti, kad kibernetinio saugumo vadovas būtų tiesiogiai atskaitingas kibernetinio saugumo subjekto vadovui ir būtų atsakingas už reikalavimų, nustatytų kibernetinio saugumo subjektui (arba keliems subjektams) dėl kibernetinio saugumo rizikų valdymo priemonių ir pranešimų apie incidentus, įgyvendinimą (KSĮ projekto 15 straipsnio 1 dalis). Kibernetinio saugumo vadovą būtų tikslinga skirti didelėse organizacijose, turinčiose nutolusių padalinių ir valdančiose ir (ar) tvarkančiose daugiau nei vieną tinklų ir informacinę sistemą arba kompleksines tinklų ir informacines sistemas. Kibernetinio saugumo vadovui galėtų būti pavaldūs kiti asmenys organizacijoje, kurie įgyvendina atskiras kibernetinio saugumo priemones arba yra atsakingi už pavienių tinklų ir informacinių sistemų saugumą.

Tuo tarpu saugos įgaliotinis, kaip ir pagal galiojančias KSĮ nuostatas, būtų atsakingas už konkrečios ryšių ir informacinės sistemos (arba kelių informacinių sistemų) kibernetinio saugumo rizikų valdymo priemonių ir pranešimų apie incidentus įgyvendinimą (KSĮ projekto 15 straipsnio 2 dalis). Siūloma taip pat įtvirtinti, kad kibernetinio saugumo vadovas galėtų vykdyti saugos įgaliotinio funkcijas, o sprendimą dėl asmenų, atsakingų už kibernetinį saugumą, skyrimo turėtų priimti esminio ir svarbaus subjekto vadovas, atsižvelgdamas į kibernetinio saugumo subjekto organizacinę struktūrą ir dydį (KSĮ projekto 15 straipsnio 3 dalis). Pažymėtina, kad kibernetinės saugos organizavimo tęstinumui išlaikyti valstybės informacinių išteklių atveju numatoma, kad tinklų ir informacinės sistemos valdytojas turi teisę pavesti tinklų ir informacinės sistemos tvarkytojui paskirti saugos įgaliotinį.

Kibernetinio saugumo subjektui taip pat leidžiama iš tiekėjo įsigyti paslaugas, kurių metu būtų vykdomos už kibernetinį saugumą atsakingų asmenų funkcijos (KSĮ projekto 15 straipsnio 4 dalis).

KSĮ projekto 15 straipsnio 5 dalimi nustatomi reikalavimai asmenims, atsakingiems už kibernetinį saugumą, išlaikant KSĮ jau nustatytus esminius reikalavimus (skiriant už kibernetinį saugumą atsakingus asmenis, jie neturėtų neišnykusio ar nepanaikinto teistumo už nusikaltimą ir negali turėti paskirtos administracinės nuobaudos tam tikrose srityse) bei siūlant įtvirtinti papildomus (įvedamas nepriekaištingos reputacijos kriterijus bei žinių ir kvalifikacijos reikalavimai). Atkreiptinas dėmesys, kad galiojančiame KSĮ esantis reikalavimas saugos įgaliotiniui neturėti neišnykusio ar nepanaikinto teistumo už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui yra integruotas į Lietuvos Respublikos valstybės tarnybos įstatyme nustatytus nepriekaištingos reputacijos kriterijus (5 straipsnio 2 dalis). Nauji siūlomi įvesti reikalavimai turėtų sustiprinti asmenų, atsakingų už kibernetinį saugumą, pozicijas kompetencijos požiūriu, mažinti riziką tapatinti informacinių technologijų valdymą su kibernetiniu saugumu bei užtikrinti, kad su kibernetiniu saugumu dirbantys asmenys būtų mažiau asmeniškai pažeidžiami. Reikalavimai už kibernetinį saugumą atsakingiems asmenims nustatomi bendri, kadangi visi minėti asmenys neturėtų turėti administracinių nuobaudų, turi būti nepriekaištingos reputacijos, taip pat turi turėti nustatytą būtinąjį kompetencijų lygį. Pažymėtina, kad atsižvelgiant į tai, kad kibernetinio saugumo vadovas galėtų vykdyti saugos įgaliotinio funkcijas, nėra tikslinga diferencijuoti reikalavimų už kibernetinį saugumą atsakingiems asmenims.

KSĮ projekto 15 straipsnio 6 dalimi nustatoma, kad fiziniam asmeniui netaikomi šiame straipsnyje nustatyti reikalavimai. Šia nuostata siekiama nesudaryti administracinės naštos fiziniam asmeniui, kuris nevykdo veiklos kaip juridinis asmuo, įsigyti rinkoje asmenų, atsakingų už kibernetinį

saugumą, paslaugas. Dėl fizinio asmens veiklos būdo išskirtinumo jis pats, būdamas kibernetinio saugumo subjektas, turėtų užtikrinti kibernetinį saugumą.

8. TIS 2 direktyvos 23 straipsnyje esminiams ir svarbiems subjektams numatoma pareiga pranešti apie bet kokį incidentą, darantį didelį poveikį subjektų vykdomai veiklai ir (ar) teikiamoms paslaugoms. Taip pat pažymėtina, kad šiuo metu KSĮ nustatyta, kad kibernetinio saugumo subjektai praneša NKSC apie jų valdomose ir (arba) tvarkomose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka, o esama incidentų klasifikavimo sistema taip pat suskirstyta į kelias kibernetinių incidentų kategorijas, atsižvelgiant į kibernetinių incidentų poveikį. Atsižvelgus į tai, kad Nacionaliniame kibernetinių incidentų valdymo plane yra nustatytos keturios kibernetinių incidentų kategorijos (pavojingi kibernetiniai incidentai, didelio poveikio kibernetiniai incidentai, vidutinio poveikio kibernetiniai incidentai, nereikšmingo poveikio kibernetiniai incidentai), bei į tai, kad kibernetinių incidentų skaičius, mastas, sudėtingumas, dažnumas ir poveikis didėja bei kelia didelę grėsmę tinklų ir informacinių sistemų veikimui, taip pat siekiant, kad būtų užtikrintas dabartinės praktikos tęstinumas ir toliau plėtojamos įgytos žinios ir patirtis, siūloma KSĮ projekto 18 straipsnio 1 dalyje nustatyti, kad esminiai ir svarbūs subjektai praneštų NKSC ne tik apie didelį kibernetinį incidentą, bet ir apie kitus kibernetinius incidentus, nustatyti išsamų pranešimo turinį, taip pat nustatyti, kad atitinkamai praneštų apie kibernetinį incidentą ir kibernetinę grėsmę Nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatyta tvarka. Numatoma peržiūrėti šiuo metu nustatytas kibernetinių incidentų kategorijas ir kriterijus ir apibrėžti kibernetinius incidentus, apie kuriuos subjektai privalėtų pranešti.

KSĮ projekto 18 straipsnio 2 dalyje siūloma apibrėžti didelį kibernetinį incidentą taip, kaip numatyta TIS 2 direktyvos 23 straipsnyje. Kibernetinis incidentas dideliu būtų laikomas, jeigu dėl jo atitinkamas subjektas patyrė arba gali patirti didelių paslaugų teikimo sutrikimų arba finansinių nuostolių arba jeigu kibernetinis incidentas paveikė arba gali paveikti kitus fizinius ar juridinius asmenis sukeldamas didelę turtinę arba neturtinę žalą. Pažymėtina, kad TIS 2 direktyvos 23 straipsnio 11 dalyje numatoma galimybė Europos Komisijos priimamuose įgyvendinimo aktuose išsamiau nustatyti pateikiamos informacijos apie didelius kibernetinius incidentus rūšis, formatus ir procedūras. Atsižvelgiant į tai, KSĮ projekte daugiau nei TIS 2 direktyvoje neplėtojama didelio kibernetinio incidento samprata, tačiau paliekama galimybė Vyriausybei tai padaryti Nacionaliniame kibernetinių incidentų valdymo plane (KSĮ projekto 18 straipsnio 6 dalies 5 punktas), jeigu nebūtų priimti atitinkami Europos Komisijos įgyvendinimo aktai.

KSĮ projekto 18 straipsnio 4 dalyje siūloma nustatyti išsamų pranešimo apie kibernetinį incidentą turinį. Siūloma nustatyti, kad kai esminiai ar svarbūs subjektai sužino apie didelį incidentą, jie nepagrįstai nedelsdami per 24 valandas turi pateikti ankstyvąjį perspėjimą. Po ankstyvojo perspėjimo turėtų būti pateikiamas pranešimas apie incidentą. Subjektai turėtų nepagrįstai nedelsdami per 72 valandas nuo tada, kai sužinojo apie didelį incidentą, pateikti pranešimą apie incidentą, visų pirma siekdami atnaujinti ankstyvuoju perspėjimu pateiktą informaciją, ir pateikti didelio incidento, įskaitant jo rimtumą ir poveikį, pradinį vertinimą, taip pat užvaldymo rodiklius, jei tokių yra. Galutinis pranešimas turėtų būti pateiktas ne vėliau kaip per vieną mėnesį nuo pranešimo apie incidentą. Ankstyvajame perspėjime turėtų būti pateikta tik ta informacija, kurios reikia, kad NKSC būtų informuotas apie didelį incidentą, o atitinkamas subjektas prireikus galėtų kreiptis pagalbos. Tokiame ankstyvajame perspėjime, turėtų būti nurodyta, ar įtariama, kad didelį incidentą sukėlė neteisėti arba piktavališki veiksmai, ir ar tikėtina, kad jis turės tarpvalstybinį poveikį.

Tuo atveju, jei galutinio pranešimo pateikimo metu incidentas tebevyksta, siūloma nustatyti, kad subjektai tuo metu pateiktų tarpinę pažangos ataskaitą, o galutinę ataskaitą – per vieną mėnesį nuo tada, kai suvaldė didelį incidentą. Kadangi reguliuojami teisiniai santykiai susiję su dideliais incidentais, priklausomai nuo aplinkybių tarpinių pažangos ataskaitų teikimo terminas galėtų būti ir labai trumpas, todėl jį numatyti įstatyme netikslinga.

KSĮ projekto 18 straipsnio 6 dalyje siūloma apibrėžti išsamesnes nuostatas apie kitus kibernetinius incidentus, kurios turi būti detaliau nustatytos Nacionaliniame kibernetinių incidentų

valdymo plane (pranešimo terminai, pranešimo turinys, informacijos apie kibernetinį incidentą pateikimo būdai ir priemonės, institucijų veiksmai).

Taip pat pažymėtina, kad nors galiojančiame KSĮ 16 straipsnyje yra nustatyta galimybė asmenims, kuriems KSĮ nėra nustatytos pareigos pranešti apie kibernetinius incidentus, savanoriškai pranešti apie kibernetinius incidentus, tačiau papildomai įvertinus tai, kad požiūris į kibernetines grėsmes yra nepaprastai svarbus kibernetinio saugumo rizikos valdymo priemonių elementas, kuris turėtų sudaryti sąlygas kompetentingoms institucijoms veiksmingai užkirsti kelią kibernetinių grėsmių tapimui incidentais, dėl kurių gali būti patiriama didelė turtinė ar neturtinė žala, ir siekiant įgyvendinti TIS 2 direktyvos 30 straipsnį dėl savanoriško pranešimo ne tik apie kibernetinius incidentus, siūloma papildyti KSĮ projekto 24 straipsnį, kad subjektams, kuriems KSĮ projekte nėra nustatytos pareigos pranešti apie kibernetinius incidentus, kibernetines grėsmes, vos neįvykusius incidentus ir (ar) taikytas kibernetinių incidentų valdymo priemones, turėtų teisę savanoriškai apie juos pranešti NKSC.

9. KSIT paskirtį siūloma plėsti. KSIT yra sistema, skirta kibernetinio saugumo subjektams, ir kurios pagrindinės funkcijos yra automatizuotai tvarkyti duomenis apie kibernetinius incidentus, apdoroti, formuoti ir paskirstyti techninių kibernetinio saugumo priemonių fiksuojamus kibernetinius incidentus pagal jų svarbos kategorijas, vykdyti kibernetinių incidentų paiešką, kaupti duomenis apie kibernetinius incidentus ir (arba) kibernetines grėsmes, tikrinti pateiktus failus dėl kenksmingo kodo ir pan. Siekiant užtikrinti dabartinės praktikos tęstinumą, kibernetinio saugumo subjektams teikti daugiau paslaugų, automatizuoti naujas NKSC atsirandančias funkcijas ir optimizuoti informacijos mainus, integraciją ir sklaidą, siūloma KSĮ projekto 19 straipsnio 1 dalies 1, 3, 4, 7 punktais praplėsti KSIT paskirtį. Siūloma patikslinti esamą reglamentavimą, kad KSIT galima būtų keistis duomenimis, susijusiais su kibernetinėmis grėsmėmis ir vos neįvykusiais incidentais (KSĮ projekto 19 straipsnio 1 dalies 5 punktas), kaip to reikalauja TIS 2 direktyva, ir atitinkamai KSIT galėtų naudotis asmenys, kurie atitinka KSIT nuostatuose nurodytus reikalavimus (KSĮ projekto 19 straipsnio 3 dalis).

Atsižvelgiant į tai, kad NKSC tampa KSIT tvarkytoju (KSĮ projekto 19 straipsnio 2 dalis), KSĮ projekto 19 straipsnio 1 dalies 1 punkte siūloma nustatyti, kad Kibernetinio saugumo subjektų registro objektai registruojami ir tvarkomi KSIT. Siekiant integruoti KSĮ nustatytą valstybės informacinių išteklių atitikties saugos reikalavimams stebėsenos sistemą į KSIT, KSĮ projekto 19 straipsnio 1 dalies 3 punkte siūloma nustatyti, kad KSIT tvarkomi duomenys, susiję su kibernetinio saugumo rizikos valdymo priemonių įgyvendinimo stebėsena. KSIT praplėtimas stebėsenos tikslui ypač svarbus ir automatizuojant duomenų iš kibernetinio saugumo subjektų surinkimą, siekiant įvertinti jų atitiktį kibernetinio saugumo reikalavimams. Siekiant kaupti duomenis apie kibernetinio saugumo subjektus, kitas įstaigas ir ūkio subjektus, kurie galėtų prisidėti prie kibernetinių incidentų valdymo, siūloma atitinkamą nuostatą dėl duomenų kaupimo KSIT nustatyti KSĮ projekto 19 straipsnio 1 dalies 4 punkte. Taip pat, siekiant įgalinti NKSC kibernetinio saugumo subjektams teikti nemokamas kibernetinio saugumo paslaugas ir priemones, siūloma atitinkamą nuostatą dėl tokių paslaugų ir priemonių teikimo per KSIT nustatyti KSĮ projekto 19 straipsnio 1 dalies 7 punkte.

Siekiant įgyvendinti TIS 2 direktyvos 29 straipsnį, siūloma KSĮ projekto 19 straipsnio 4 dalyje nustatyti, kad kibernetinio saugumo subjektai turi teisę naudotis KSIT įgyvendindami tarpusavio dalijimosi kibernetinio saugumo informacija susitarimus. Taip pat nustatyti, kad, nepriklausomai nuo to, ar naudojamasi KSIT, kibernetinio saugumo subjektai privalėtų pranešti NKSC apie tokių susitarimų sudarymą, taip pat apie pasitraukimą iš tokių susitarimų per 20 darbo dienų nuo šių aplinkybių atsiradimo.

KSĮ projekto 19 straipsnio 5 dalyje nustatomi atvejai, kada KSIT duomenys gali būti teikiami. Išlaikant KSĮ nuostatas ir siekiant sudaryti sąlygas kibernetinį saugumą įgyvendinančioms institucijoms efektyviai atlikti joms priskirtas funkcijas, papildomai nustatomos išimtys, susijusios su incidentų tyrimu ir kibernetinio saugumo subjektų registravimu (KSĮ projekto 19 straipsnio 5 dalies 3, 4, 6 punktai).

Papildymai, susiję su KSIT, turėtų padėti subjektams bendrai naudotis savo asmeninėmis žiniomis ir praktika strateginiu, taktiniu ir operatyviniu lygmenimis, kad sustiprintų savo gebėjimus

tinkamai užkirsti kelią kibernetiniams incidentams, juos atskleisti, į juos reaguoti, atkurti veiklą po jų arba sumažinti jų poveikį.

10. Esminių spragų paieškos ir atskleidimo reglamentavimo pakeitimų nenumatoma. TIS 2 direktyvos 12 straipsnio reikalavimai iš esmės buvo įgyvendinti dar 2019 m., KSĮ 17 straipsnyje įtvirtinus atsakingo spragų atskleidimo modelį ir pavedus NKSC koordinuoti spragų atskleidimą. KSĮ projekte siekiama patikslinti galiojančias nuostatas.

KSĮ projekto 7 straipsnio 2 dalies 10 punkte nustatoma, kad NKSC koordinuoja spragų atskleidimą. Siekiant įgyvendinti TIS 2 direktyvos 12 straipsnio 1 dalies 2 paragrafą, KSĮ projekto 25 straipsnio 3 dalyje nustatoma, kad asmuo, surinkęs informaciją apie spragą, turi teisę šią informaciją anonimiškai pateikti NKSC (NKSC užtikrina apie spragą pranešusio subjekto anonimiškumą), išsaugodamas nacionalinės spragų atskleidimo tvarkos apraše nurodytą informaciją apie spragų paieškos rezultatų pateikimą. Atsižvelgiant į TIS 2 direktyvos reikalavimą dėl anonimiškumo ir siekiant išlaikyti siekį spragų ieškoti teisėtu būdu pagal KSĮ nustatytas sąlygas, nustatoma, kad anonimiškai spragą atskleidžiantis asmuo turi saugoti informaciją apie spragų paieškos rezultatų pateikimą 12 metų nuo pranešimo NKSC pateikimo dienos. Šis informacijos saugojimo reikalavimas nustatomas atsižvelgiant į KSĮ nustatytas spragų ieškojimo sąlygas ir Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje numatytoms nusikalstamoms veikoms taikomus senaties terminus. Kadangi KSĮ nustatytų spragų ieškojimo sąlygų nesilaikymas sukuria pagrindą taikyti baudžiamąją atsakomybę, asmuo turėtų išsaugoti duomenis, įrodančius, kad spragų buvo ieškoma teisėtai. Pavyzdžiui, KSĮ projekto 25 straipsnio 2 dalies 3 punkte numatoma pareiga visiems asmenims, ieškojusiems spragų, apie vykdytą spragų paieška pranešti NKSC arba atitinkamam subjektui, kurio tinklų ir informacinėse sistemose buvo ieškoma spragų, – to nepadarius formaliai kyla pagrindas taikyti baudžiamąją atsakomybę. NKSC užtikrinus galimybę apie spragas informuoti anonimiškai, NKSC negalėtų patvirtinti, kad būtent konkretus asmuo įgyvendino KSĮ projekto 25 straipsnio 2 dalies 3 punkte numatytą pareigą. Dėl vienokių ar kitokių priežasčių pradėjus ikiteisminį tyrimą ir kitais būdais (nesusijusiais su galimybe pranešti apie spragą anonimiškai) nustačius asmenį, ieškojusi spragų, turėtų būti sudarytos prielaidos šiam asmeniui apsiginti nuo nepagrįsto baudžiamojo persekiojimo. Šios prielaidos ir sukuriamos nustatant įpareigojimą pačiam asmeniui saugoti informaciją apie jo atliktą spragų paiešką.

Siekiant apriboti spragą atskleidusio asmens galimybes imtis bet kokių veiksmų su atskleistais asmens duomenimis, KSĮ projekto 25 straipsnio 2 dalies 5 punkte nustatoma papildoma sąlyga nenaudoti pastebėtų, užfiksuotų, perimtų, atskleistų asmens duomenų.

Siekiant įgyvendinti TIS 2 direktyvos 12 straipsnio 2 dalį, KSĮ projekto 25 straipsnio 2 dalies 7 punkto sąlyga nesidalinti informacija apie aptiktą spragą papildoma išlyga, kad informacija dalintis galima, kai informacija apie aptiktą spragą yra registruojama Europos pažeidžiamumų duomenų bazėje.

11. Dėl tarpinstitucinio bendradarbiavimo ir savitarpio pagalbos. Atsižvelgus į tai, kad tarpinstitucinis ir taprvalstybinis bendradarbiavimas ypač svarbus siekiant veiksmingai įgyvendinti KSĮ projekto nuostatas, taip pat siekiant sudaryti sąlygas sklandžiam tarpsektoriniam bendradarbiavimui su kitomis kompetentingomis institucijomis, KSĮ projekto 20 straipsnyje numatoma nustatyti bendradarbiavimo pagrindus.

KSĮ projekto 20 straipsnio 1 dalyje siūloma nustatyti, kad kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos bendradarbiauja tarpusavyje bei su kitomis valstybės institucijomis, įskaitant Ryšių reguliavimo tarnybą, kompetentingas institucijas pagal Reglamentą (ES) Nr. 910/2014 ir Reglamentą (ES) 2022/2554, taip pat su Krizių valdymo centru, įgyvendindamos šiame įstatyme nustatytus tikslus, įskaitant keitimąsi informacija apie incidentus, kibernetines grėsmes ir vos neįvykusius incidentus.

KSĮ projekto 20 straipsnio 2 dalyje siūloma nustatyti, kad NKSC teikia pagalbą ar informuoja Nacionalinį krizių valdymo centrą (KSĮ projekto 20 straipsnio 2 dalies 1 punktas), kompetentingą instituciją, paskirtą pagal Reglamentą 2022/2554 (KSĮ projekto 20 straipsnio 2 dalies 2 ir 3 punktai), Valstybinę duomenų apsaugos inspekciją (KSĮ projekto 20 straipsnio 2 dalies 4 punktas) dėl vykdymo užtikrinimo priemonių taikymo tam tikrų subjektų atžvilgiu, siekiant užtikrinti, kad laikytųsi KSĮ

projekto reikalavimų. KSĮ projekto 20 straipsnio 2 dalies 4 punkte nustatoma, kad NKSC bendradarbiauja su Ryšių reguliavimo tarnyba dėl patikimumo užtikrinimo paslaugų teikėjų kibernetinio saugumo audito srityje. KSĮ projekto 20 straipsnio 2 dalies 5, 6 ir 7 punktuose siūloma nustatyti, kad NKSC bendradarbiauja su kitų valstybių narių kompetentingomis institucijomis, kai kibernetinio saugumo subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje arba teikia paslaugas vienoje ar daugiau valstybių narių, o jo tinklų ir informacinės sistemos yra vienoje ar daugiau kitų valstybių narių, vykdydami savitarpio pagalbos prašymus ir informuodami apie taikytiną vykdymo užtikrinimo priemonę.

Siekiant įgyvendinti TIS 2 direktyvos 37 straipsnį, siūloma KSĮ projekto 21 straipsnyje nustatyti, kad NKSC, gavęs kitos valstybės narės kompetentingos institucijos pagrįstą savitarpio pagalbos prašymą, vykdo KSĮ projekto 26 ir 28 straipsniuose numatytus kibernetinio saugumo subjektų patikrinimo ir (ar) vykdymo užtikrinimo priemonių veiksmus. Siūloma taip pat nustatyti, kokiais atvejais NKSC, gavęs kitos valstybės narės kompetentingos institucijos savitarpio pagalbos prašymą, galėtų atmesti tokį prašymą arba, jeigu prašymas pateiktas ne pagal kompetenciją, perduoti šį prašymą kitai valstybės institucijai. KSĮ projekto 22 straipsnyje detalizuojamos KSĮ nuostatos dėl nacionalinių ir tarptautinių informacijos mainų sąlygų, siekiant užtikrinti tiek asmens duomenų, tiek subjektų valdomos konfidencialios informacijos saugumą. Atsižvelgiant į tai, kad šiuo metu nėra prašymų nagrinėjimo praktikos, sudėtinga įvertinti, kiek laiko gali prireikti nagrinėjant prašymuose nurodytas aplinkybes, todėl savitarpio pagalbos prašymų nagrinėjimo, persiuntimo, pranešimo apie persiuntimą bei atsisakymo nagrinėti (atmetimo) ir grąžinimo terminai įstatymu nenustatomi.

12. Kibernetinio saugumo subjektų patikrinimo reglamentavimas, atsižvelgiant į TIS 2 direktyvos 32 straipsnio 2 dalį bei 33 straipsnio 2 dalį, detalizuojamas ir plečiamas. Siūloma KSĮ projekto 26 straipsnyje nustatyti NKSC teisę pradėti esminio subjekto patikrinimą bet kokiu klausimu, susijusiu su KSĮ projekte nustatytais reikalavimais, kurių nevykdymas laikomas pažeidimu. Esminiams ir svarbiems subjektams taikomi patikrinimo režimai diferencijuojami siekiant nedidinti administracinės naštos. Esminiams subjektams taikoma išsami *ex ante* ir *ex post* priežiūros tvarka, o svarbiems subjektams taikoma negriežta, tik *ex post*, priežiūros tvarka. Svarbių subjektų patikrinimas turėtų būti pradedamas tik gavus duomenų ar informacijos, kad svarbus subjektas, kaip įtariama, padarė KSĮ nustatytų reikalavimų pažeidimą.

KSĮ 27 straipsnyje siūloma nustatyti bendrąsias kibernetinio saugumo subjektų patikrinimų atlikimo taisykles, susijusias su patikrinimo trukme, NKSC ir jo darbuotojų teisėmis. NKSC patikrinimus atliktų KSĮ 27 straipsnyje ir NKSC nustatyta tvarka. Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 2 dalį bei 33 straipsnio 2 dalį, siūloma KSĮ projekto 27 straipsnio 3 dalyje nustatyti šias NKSC teises: 1) įgalioti asmenis, turinčius teisę įeiti į kibernetinio saugumo subjektų patalpas, ne ilgesniam kaip 30 kalendorinių dienų terminui paimti dokumentų kopijas ir nuorašus, duomenų kopijas bei kitus daiktus, reikalingus atliekant patikrinimus; 2) duoti nurodymus kibernetinio saugumo subjektams savo lėšomis atlikti nepriklausomą tinklų ir informacinių sistemų arba jomis vykdomos veiklos ar teikiamų paslaugų tikslinį saugumo auditą; 3) duoti nurodymus pateikti visą reikalingą informaciją, dokumentų kopijas ir išrašus; 4) duoti nurodymus pateikti žodinius ir rašytinius paaiškinimus; 5) patikrinimui atlikti savo lėšomis pasitelkti specialistų ir ekspertų; 6) sudaryti sutartis su audito įmonėmis, kitais subjektais, kurių paslaugomis NKSC naudosis atlikdamas patikrinimą; 7) naudoti visą NKSC turimą informaciją; 8) naudotis kitomis įstatymų suteiktomis teisėmis. Siekiant užtikrinti patikrinimų veiksmingumą ir efektyvumą NKSC atliekant patikrinimus, siūloma to paties straipsnio 4 dalyje nustatyti teises įeiti į kibernetinio saugumo subjektų patalpas, užfiksuoti faktines aplinkybes, naudoti technines priemones, tikrinti asmenų tapatybę patvirtinančius dokumentus.

KSĮ 27 straipsnio 7 ir 8 dalyse siūloma nustatyti patikrinimo pabaigoje priimamus sprendimus bei nustatyti sąlygas, kada taikyti teisę taikyti KSĮ 28 straipsnyje nustatytas vykdymo užtikrinimo priemones.

13. Dėl vykdymo užtikrinimo priemonių. Siekiant įgyvendinti TIS 2 direktyvos 32 straipsnio 4 ir 5 dalis bei 33 straipsnio 4 dalį, siūloma KSĮ projekto 28 straipsnyje nustatyti toliau aprašomas

vykdymo užtikrinimo priemones, kurios būtų taikomos NKSC nustačius KSĮ projekto 29 straipsnyje nurodytus pažeidimus.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 4 dalies a punktą bei 33 straipsnio 4 dalies a punktą, kuriuose nustatoma, kad kompetentinga institucija turi turėti įgaliojimą teikti įspėjimus, kai atitinkami subjektai pažeidžia nustatytus reikalavimus, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 1 dalies 1 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 4 dalies b punktą bei 33 straipsnio 4 dalies b punktą, kuriuose nustatoma, kad kompetentinga institucija turi turėti įgaliojimą priimti privalomus nurodymus, kuriuo reikalaujama, kad atitinkami subjektai pašalintų nustatytus trūkumus arba ištaisytų pažeidimą, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 1 dalies 2 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 4 dalies c punktą bei 33 straipsnio 4 dalies c punktą, kuriuose nustatoma, kad kompetentinga institucija turi turėti įgaliojimą nurodyti atitinkamiems subjektams nutraukti veiksmus, kurie pažeidžia KSĮ, ir tokių veiksmų nebekartoti, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 1 dalies 3 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 4 dalies d punktą bei 33 straipsnio 4 dalies d punktą, kuriuose nustatoma, kad kompetentinga institucija turi turėti įgaliojimą nurodyti atitinkamiems subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų kibernetinio saugumo rizikos valdymo priemonės atitiktų TIS 2 direktyvos 21 straipsnį arba kad jie įvykdytų TIS 2 direktyvos 23 straipsnyje nustatytas pareigas nurodyti atitinkamiems subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų kibernetinio saugumo rizikos valdymo priemonės atitiktų TIS 2 direktyvos 21 straipsnį arba kad jie įvykdytų TIS 2 direktyvos 23 straipsnyje nustatytas pareigas pranešti, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 1 dalies 4 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 4 dalies e punktą bei 33 straipsnio 4 dalies e punktą, kuriuose nustatoma, kad kompetentinga institucija turi turėti įgaliojimą įpareigoti atitinkamus subjektus informuoti subjektus, kuriems jie teikia paslaugas arba vykdo veiklą ir kuriuos gali paveikti didelė kibernetinė grėsmė, apie grėsmės pobūdį, taip pat apie visas galimas apsaugos ar taisomąsias priemones, kurių gali imtis tie fiziniai ar juridiniai asmenys, reaguodami į tą grėsmę, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 1 dalies 5 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 4 dalies f punktą bei 33 straipsnio 4 dalies f punktą, kuriuose nustatoma, kad kompetentinga institucija turi turėti įgaliojimą įpareigoti atitinkamus subjektus per pagrįstą terminą įgyvendinti saugumo audito metu pateiktas rekomendacijas, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 1 dalies 6 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 4 dalies h punktą bei 33 straipsnio 4 dalies g punktą, kuriuose nustatoma, kad kompetentinga institucija turi turėti įgaliojimą įpareigoti atitinkamus subjektus konkrečiu būdu viešai paskelbti KSĮ pažeidimo aspektus, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 1 dalies 8 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 4 dalies g punktą, kuriame nustatoma, kad kompetentinga institucija turi turėti įgaliojimą paskirti stebėsenos pareigūną, kuriam per nustatytą laikotarpį pavestos aiškiai apibrėžtos užduotys, prižiūrėti, kaip atitinkami subjektai laikosi TIS 2 direktyvos 21 ir 23 straipsnių, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 1 dalies 7 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 4 dalies i punktą bei 33 straipsnio 4 dalies h punktą, kuriuose nustatoma, kad kompetentinga institucija turi turėti įgaliojimą skirti arba prašyti, kad atitinkamos įstaigos ar teismai pagal nacionalinę teisę skirtų administracinę baudą pagal TIS 2 direktyvos 34 straipsnį, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 1 dalies 9 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 5 dalies a punktą, kuriame nustatoma, kad kompetentinga institucija turi turėti įgaliojimą laikinai sustabdyti arba prašyti, kad sertifikavimo arba leidimus išduodanti įstaiga, arba teismas pagal nacionalinę teisę laikinai sustabdytų sertifikavimą arba įgaliojimą, susijusį su dalimi arba visomis esminio subjekto teikiamomis atitinkamomis paslaugomis

ar vykdoma veikla, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 1 dalies 10 punkte bei 32 straipsnyje.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 5 dalies b punktą, kuriame nustatoma, kad kompetentinga institucija turi turėti įgaliojimą reikalauti, kad atitinkamos įstaigos arba teismai pagal nacionalinę teisę nustatytų laikiną draudimą bet kuriam esminiame subjekte generalinio direktoriaus ar teisinio atstovo lygmens vadovaujamas pareigas einančiam fiziniam asmeniui eiti vadovaujamas pareigas tame subjekte, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 1 dalies 11 punkte bei 33 straipsnyje su išimtimi Lietuvos Respublikos Seimo, Vyriausybės ir Prezidento sprendimu skiriamiems viešojo administravimo subjektų vadovams. Nurodyta išimtimi, iš dalies taikant TIS 2 direktyvos 32 straipsnio 5 dalyje numatytą išimtį viešojo administravimo subjektams, siekiama užtikrinti, kad nebūtų įsiterpta iš aukščiausiųjų valstybės valdymo subjektų įgaliojimus, kylančius tiek iš Lietuvos Respublikos Konstitucijos (pavyzdžiui, ministrų skyrimas), tiek iš ES teisės kildinamų reikalavimų (pavyzdžiui, reikalavimai užtikrinti nacionalinio centrinio banko nepriklausomumą).

Taip pat KSĮ projekto 28 straipsnio 7 dalyje nustatoma, kad sprendimas dėl vykdymo užtikrinimo priemonės skyrimo gali būti priimtas, jeigu praėjo ne daugiau kaip 2 metai nuo pažeidimo dienos.

TIS 2 direktyvos 32 straipsnio 7 dalyje bei 33 straipsnio 5 dalyje nustatomos aplinkybės, kurios vertinamos patikrinimo metu parenkant efektyviausią vykdymo užtikrinimo priemonę. Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 7 dalies a punktą, kuriame nustatoma, kad patikrinimo metu turi būti atsižvelgiama į pažeidimo sunkumą ir pažeistų nuostatų svarbą siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 3 dalies 1 punkte ir 5 dalyje. TIS 2 direktyvos 32 straipsnio 7 dalies a punkto papunkčiuose nustatoma, kad sunkiais pažeidimais laikomi pakartotiniai pažeidimai, nepranešimas apie didelius incidentus, trūkumų pagal kompetentingų institucijų privalomus vykdyti nurodymus neištaisymas, trukdymas vykdyti audito ar stebėsenos veiklą, kurią įpareigojo atlikti kompetentinga institucija nustačius pažeidimą, neteisingos ar labai netikslios informacijos, susijusios su kibernetinio saugumo rizikos valdymo priemonėmis arba pareigomis pranešti, nustatytomis TIS 2 direktyvos 21 ir 23 straipsniuose, pateikimas. Šios aplinkybės nustatomos KSĮ projekto 28 straipsnio 5 dalyje kaip atsakomybę sunkinančiomis. Atitinkamai, atsižvelgiant į Konstitucinio Teismo doktriną bei TIS 2 direktyvoje nustatytą pareigą atsižvelgti į kiekvieno konkretaus atvejo aplinkybes numatomos ir atsakomybę lengvinančios aplinkybės skatinančios kibernetinio saugumo subjektus mažinti žalą, bendradarbiauti su NKSC, taip pat kitas aplinkybes susijusias su subjekto tyčios nebuvimu. Pažymėtina, kad siekiant nustatyti aiškias sąlygas, kada pažeidimas laikomas padarytas pakartotinai, nustatomas 12 mėnesių terminas nuo sprendimo, kuriuo buvo paskirta vykdymo užtikrinimo priemonė, įsigaliojimo dienos. Šiuo laikotarpiu įvykdytas toks pat pažeidimas laikomas padarytu pakartotinai. Taip pat, siekiant mažinti riziką, kai kibernetinio saugumo subjektai ignoruoja ar nepaiso NKSC įspėjimų ir nurodymų, siūloma nustatyti, kad sunkiu pažeidimu laikomas padaryto pažeidimo slėpimas, pažeidimo tęsimas, nepaisant to, kad NKSC buvo atkreipęs dėmesį į pažeidimus ar veiklos trūkumus (KSĮ projekto 28 straipsnio 4 dalies 6 punktas). Atsižvelgiant į pažeidimų suskirstymą pagal sunkumą (aprašoma tekste žemiau), sunkiais pažeidimais taip pat laikomi KSĮ projekto 29 straipsnio 2 dalyje nustatyti pažeidimai.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 7 dalies b punktą, kuriame nustatoma, kad patikrinimo metu turi būti atsižvelgiama į pažeidimo trukmę, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 3 dalies 2 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 7 dalies c punktą, kuriame nustatoma, kad patikrinimo metu turi būti atsižvelgiama į atitinkamo subjekto įvykdytus svarbius ankstesnius pažeidimus, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 3 dalies 3 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 7 dalies d punktą, kuriame nustatoma, kad patikrinimo metu turi būti atsižvelgiama į padarytą turtinę arba neturtinę žalą, įskaitant finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms ir paveiktų naudotojų skaičių, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 3 dalies 4 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 7 dalies e punktą, kuriame nustatoma, kad patikrinimo metu turi būti atsižvelgiama į tai, ar pažeidimą įvykdęs asmuo veikė tyčia ar dėl neatsargumo, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 3 dalies 5 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 7 dalies f punktą, kuriame nustatoma, kad patikrinimo metu turi būti atsižvelgiama į priemones, kurių subjektas ėmėsi siekdamas užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 3 dalies 6 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 7 dalies g punktą, kuriame nustatoma, kad patikrinimo metu turi būti atsižvelgiama į patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 3 dalies 7 punkte.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 7 dalies h punktą, kuriame nustatoma, kad patikrinimo metu turi būti atsižvelgiama į atsakingais laikomų fizinių ar juridinių asmenų bendradarbiavimo su kompetentingomis institucijomis lygį, siūloma atitinkamą nuostatą nustatyti KSĮ projekto 28 straipsnio 3 dalies 8 punkte.

KSĮ projekto 28 straipsnio 3 dalies 9 punkte nustatoma aplinkybė dėl pažeidimo masto.

Atsižvelgiant į TIS 2 direktyvos 36 straipsnio nuostatą, pagal kurią valstybės narės turi nustatyti sankcijas, taikomas pažeidus pagal TIS 2 direktyvą priimtas nacionalines nuostatas, taisykles ir turi imtis visų būtinų priemonių užtikrinti, kad šios sankcijos būtų įgyvendinamos, KSĮ projekte pažeidimai suskirstomi pagal pavojingumą, tai sudaro sąlygas diferencijuoti reikalavimų įgyvendinimo svarbą ir nustatyti priežiūros prioritetus. Pažymėtina, kad TIS 2 direktyvoje prioritetu laikomas 21 ir 23 straipsniuose nustatytų reikalavimų dėl kibernetinio saugumo rizikos valdymo priemonių ir pranešimų apie didelius incidentus įgyvendinimas, todėl KSĮ projekto 29 straipsnyje nustatytų pavojingų pažeidimų grupei priskiriami atitikties kibernetinio saugumo rizikos valdymo priemonėms nevykdymas ar netinkamas vykdymas, informacijos apie didelį kibernetinį incidentą neteikimas

Vidutinio pavojingumo pažeidimais laikomi pažeidimai, susiję su kibernetinio saugumo politiką įgyvendinančių institucijų nurodymų nevykdymu ar netinkamu vykdymu. KSĮ projekto 7 straipsnio 2 dalies 6 ir 7 punktuose nustatytas NKSC nurodymo teikimas tam tikrai kibernetinio saugumo subjektų grupei. Šie nurodymai kritiškai svarbūs siekiant laiku sustabdyti vykstantį kibernetinį incidentą ar kitą žalingą veiklą kibernetinėje erdvėje ir sudaro sąlygas maksimaliai mažinti keliamą žalą. KSĮ projekto 27 straipsnio 3 dalyje nustatytos NKSC teisės, taikomos patikrinimų metu. Šių reikalavimų nevykdymas ar netinkamas vykdymas, nesudarymas sąlygų NKSC įgyvendinti teises laikomi vidutinio pavojingumo pažeidimais, kadangi sudaro sąlygas kibernetinio saugumo subjektams sutrukdyti NKSC laiku identifikuoti didesnio masto ir didesnę žalą sukeliančius pažeidimus. KSĮ projekto 14 straipsnio 6 ir 8 dalyse nustatytas įpareigojimas kibernetinio saugumo subjekto vadovui arba jo įgaliotam asmeniui užtikrinti, kad kibernetinio saugumo subjektas laikytųsi įstatyme jam nustatytų pareigų, ir prižiūrėti jų laikymąsi bei prievolė ne rečiau kaip kartą per 3 metus atlikti kibernetinio saugumo auditą. KSĮ projekto 15 straipsnio 1, 2 ir 3 dalyse nustatyti reikalavimai paskirti už kibernetinį saugumą atsakingus asmenis. Šių reikalavimų pažeidimai priskiriami vidutinio pavojingumo pažeidimams, nes jų nevykdymas ar netinkamas vykdymas kelia riziką dėl didesnio masto ir didesnę žalą sukeliančių pasekmių atsiradimo. Kibernetinio saugumo subjekto vadovo atsakomybės už kibernetinį saugumą suvokimas, už kibernetinį saugumą atsakingų asmenų paskyrimas, reguliarus kibernetinių rizikų identifikavimas auditų metu yra esminė ir būtinoji sąlygą užtikrinti nuoseklios, tęstinės kibernetinio saugumo politikos organizacijoje palaikymą ir brandos didinimą. KSĮ projekto 17 straipsnyje nustatytų reikalavimų aukščiausio lygio domenų vardų registravimo paslaugas teikiantiems subjektams pažeidimai priskiriami vidutinio pavojingumo pažeidimams dėl jų teikiamos paslaugos kritiškumo.

Nedidelio pavojingumo pažeidimais laikomi pažeidimai, susiję su informuotumo, nedarančio įtakos kibernetinio saugumo būklės ir rizikų vertinimui, neužtikrinimu ar netinkamu užtikrinimu. KSĮ projekto 14 straipsnio 3 dalyje numatytas įpareigojimas kibernetinio saugumo subjektams pateikti duomenis apie kibernetinio saugumo rizikos valdymo priemonių įgyvendinimą, to paties straipsnio 7

dalyje nustatytas reikalavimas dėl kibernetinio saugumo subjekto vadovo mokymosi. Šių reikalavimų pažeidimai tiesiogiai nekelia rizikų kibernetinio saugumo būklei organizacijoje, nėra susiję su kritinėse situacijose atliktinais veiksmais. KSĮ projekto 18 straipsnio 1 dalies 2 punkte nustatytas įpareigojimas kibernetinio saugumo subjektams pranešti NKSC apie kitus, ne didelius, kibernetinius incidentus. Esamame reglamentavime nėra reikalaujama skubiai pranešti apie tokio pobūdžio incidentus, todėl pranešimas apie juos laikomas ne skubiu, bet svarbiu veiksniu bendram grėsmių situacijos vaizdui konstruoti. KSĮ projekto 19 straipsnio 4 dalyje nustatytas įpareigojimas kibernetinio saugumo subjektams pranešti NKSC apie tarpusavio dalijimosi kibernetinio saugumo informacija susitarimus taip pat laikomas informaciniu įpareigojimu, skirtu bendram žinojimui konstruoti. KSĮ projekto 17 straipsnyje nustatytų reikalavimų domenų vardų registravimo paslaugas teikiantiems subjektams pažeidimai priskiriami nedidelio pavojingumo pažeidimams, nes TIS 2 direktyva nėra linkusi nustatyti didelės apimties reikalavimų, atitinkamai vykdymo užtikrinimo veiksmų šiems subjektams.

Siekiant įgyvendinti TIS 2 direktyvos 34 ir 36 straipsnius, siūloma KSĮ projekto 30 straipsnyje nustatyti baudų dydžius, juos susiejant su pažeidimo pavojingumu. KSĮ projekto 30 straipsnio 1 dalyje siūloma nustatyti, kad baudas skiria NKSC vadovas ar jo įgaliotas asmuo pagal vykdymo užtikrinimo priemonių taikymo esminiams ir svarbiems subjektams tvarką, tvirtinamą Vyriausybės.

Viena iš NKSC taikomų vykdymo užtikrinimo priemonių yra baudų skyrimas. TIS 2 direktyvos 34 straipsnyje esminiams subjektams nustatoma bauda iki 10 000 000 Eur arba iki 2 proc. juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri yra didesnė, svarbiems subjektams nustatoma bauda iki 7 000 000 Eur arba iki 1,4 proc. juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri yra didesnė. Šios nuostatos išdėstomos atitinkamai KSĮ projekto 30 straipsnio 2 dalies 1 ir 2 punktuose.

Vertinant administracinių baudų skyrimą valdžios institucijoms ir įstaigoms buvo vertinti keli galimi modeliai: valdžios institucijoms ir įstaigoms neskirti TIS 2 direktyvos numatytų administracinių baudų (pvz., taip savo įstatymuose ketina nustatyti Kroatija, Belgija); skirti tokias pačias, kaip ir kitiems subjektams; nustatyti kitokio dydžio baudas. KSĮ 30 straipsnio 3 dalies 3 ir 4 punktuose siūloma nustatyti mažesnes baudų valdžios institucijoms ir įstaigoms viršutines ribas, siekiant turėti priemonę drausminti valdžios institucijas ir įstaigas, bet kartu nesukelti didelio pavojaus, kad, pritaikius maksimalų baudos dydį, bus sutrikdyta jų veikla ir prireiks perskirstyti valstybės biudžetą (institucija galimai įstengtų tokio dydžio baudas sumokėti iš jai skirtų asignavimų). Valdžios institucijoms ar įstaigoms KSĮ projekto 30 straipsnio 2 dalies 3 punkte nustatomas baudos dydis iki 1 procento valdžios institucijos ar įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė negu 60 000 Eur esminiam subjektui, ir KSĮ projekto 30 straipsnio 2 dalies 4 punkte – iki 0,5 procento valdžios institucijos ar įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė negu 30 000 Eur svarbiam subjektui.

Vertinant administracinių baudų skyrimo modelį buvo vertinti keli galimi variantai: KSĮ nustatyti tik maksimalias baudas arba labiau detalizuojant susieti baudų dydžius su pažeidimų pavojingumu. Siekiant nustatyti aiškesnį baudų skyrimo reglamentavimą, pasirinkta baudų dydžius sieti su pažeidimų pavojingumu. Baudų skyrimo modelis remiasi baudų dydžio nustatymu atsižvelgiant į pažeidimo pavojingumą. Nustatomos trys pažeidimų pavojingumo kategorijos, kiekvienai iš kategorijų nustatant maksimalią baudos ribą. Atsižvelgiant į tai, kad nustatomos trys pažeidimų pavojingumo kategorijos, maksimalios baudos ribos kiekvienai kategorijai išdėstomos proporcingai: 100 proc. skalėje pavojingiems pažeidimams nustatoma iki 100 proc. TIS 2 direktyvos 34 straipsnyje nustatytos maksimalios baudos, vidutinio pavojingumo pažeidimams nustatoma iki 50 proc. TIS 2 direktyvos 34 straipsnyje nustatytos maksimalios baudos ir nedidelio pavojingumo pažeidimams nustatoma iki 10 proc. TIS 2 direktyvos 34 straipsnyje nustatytos maksimalios baudos. Šios nuostatos išdėstomos KSĮ 30 straipsnio 3 dalies 1–3 punktuose. KSĮ 30 straipsnio 1 dalyje nustatyta, kad baudas skiria NKSC vadovas ar jo įgaliotas asmuo pagal Vykdymo užtikrinimo priemonių taikymo esminiams ir svarbiems subjektams tvarką, tvirtinamą Vyriausybės.

TIS 2 direktyvos 32 straipsnio 6 dalyje ir 33 straipsnio 6 dalyje nustatyti reikalavimai, kad fizinis asmuo, atsakingas už esminį ar svarbų subjektą arba veikiantis kaip jo teisinis atstovas, remdamasis jam suteiktais įgaliojimais atstovauti tam subjektui, įgaliojimu priimti sprendimus jo vardu arba įgaliojimu vykdyti jo kontrolę, turėtų įgaliojimus užtikrinti, kad subjektas laikytųsi TIS 2 direktyvos, bei numatyta galimybė šiuos asmenis traukti atsakomybėn už jų pareigų nesilaikymą. Atsižvelgiant į tai, ANK projekte juridinių asmenų vadovams ar kitiems atsakingiems asmenims nustatoma bauda už KSĮ nustatytų reikalavimų pažeidimą nuo 250 iki 3000 Eur, o nusižengimas, padarytas pakartotinai, užtraukia baudą nuo 2000 iki 6000 Eur.

KSĮ projekte taip pat būtina nustatyti baudos skyrimo procedūrą. KSĮ projekto 31 straipsnio 1–13 dalyse nustatomos baudos skyrimo procedūra bei sprendimo dėl baudos skyrimo vykdymo tvarka. Nustatoma, kad baudos skyrimas gali būti svarstomas rašytinės procedūros tvarka (KSĮ projekto 31 straipsnio 1 ir 8 dalys) arba žodinės procedūros tvarka rengiant posėdį (KSĮ projekto 31 straipsnio 2–7 dalys). Nustatoma, kad administracinės baudos skyrimo svarstymas yra viešas arba uždaras (KSĮ projekto 31 straipsnio 5 dalis), posėdis vyksta lietuvių kalba (KSĮ projekto 31 straipsnio 6 dalis), daromas posėdžio garso įrašas (KSĮ projekto 31 straipsnio 7 dalis), nustatomos sprendimo dėl administracinės baudos skyrimo sudėtinės dalys (KSĮ projekto 31 straipsnio 9 dalis), nustatomas sprendimo dėl administracinės baudos skyrimo įvykdymo terminas (KSĮ projekto 31 straipsnio 11 dalis), sprendimo dėl administracinės baudos skyrimo apskundimo tvarka (KSĮ projekto 31 straipsnio 10 dalis). KSĮ projekto 31 straipsnio 12 dalyje nustatoma, kad sprendimas dėl administracinės baudos skyrimo yra vykdomasis dokumentas, vykdomas Lietuvos Respublikos civilinio proceso kodekso nustatyta tvarka. Atsižvelgiant į TIS 2 direktyvos 35 straipsnį, siūloma KSĮ projekto 31 straipsnio 13 dalyje nustatyti, kad bauda neskiriama, jeigu kibernetinio saugumo subjektui už tą patį pažeidimą jau buvo skirta bauda vadovaujantis Reglamento 2016/679 58 straipsnio 2 dalies i punktu.

Atsižvelgiant į TIS 2 direktyvos 32 straipsnio 5 dalį, siūloma KSĮ projekto 32 ir 33 straipsniuose nustatyti atitinkamai laikino teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar paslaugų teikimu sustabdymo tvarką ir esminio subjekto vadovo laikino nušalinimo nuo pareigų tvarką. Pažymėtina, kad laikinas sustabdymas teise užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas bei laikinai nušalinti esminio subjekto vadovą nuo pareigų gali būti taikomi tik pavojingų pažeidimų atvejais. Šios vykdymo užtikrinimo priemonės įgyvendinamos teismo nutartimi, NKSC pateikus prašymą teismui. Atsižvelgiant į numatomų apribojimų pobūdį, susijusį su asmenų teisėmis pasirinkti darbą bei verslą, šios vykdymo užtikrinimo priemonės būtų taikomos kreipiantis į bendrosios kompetencijos teismus. KSĮ projekto 32 straipsnio 4 dalyje numatytas laikino juridinio asmens veiklos sustabdymo terminas, kuris negali būti ilgesnis kaip 4 mėnesiai su galimu pratęsimu. Šis terminas sietinas su KSĮ projekto 27 straipsnio 1 dalyje nurodytu patikrinimo atlikimo terminu, kuris taip pat yra 4 mėnesiai nuo skundo gavimo dienos ar sprendimo atlikti patikrinimą dienos. Papildomai pažymėtina, kad laikinas teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas sustabdymas įstatymo kontekste jau pats savaime yra numatytas kaip *ultima ratio* priemonė, kai kitos priemonės neveikia. Įvertinus tai, laikytina, kad papildomai atskiros nuostatos dėl vienos vykdymo užtikrinimo priemonės keitimo kita nereikia – sustabdymas bet kokiu atveju bus naikinamas, kai ši priemonė pasidarys nebereikalinga.

14. Siekiant įgyvendinti Reglamento nuostatas, susijusias su Kibernetinio saugumo kompetencijos bendruomenės narių registravimu (Reglamento 8 str. 3 d.), siūloma KSĮ projekto 23 straipsnio 1 dalyje nustatyti, kad Kibernetinio saugumo kompetencijos bendruomenės nariais gali tapti tik Lietuvos Respublikoje registruoti juridiniai asmenys. Jie turi įrodyti galintys prisidėti vykdant misiją ir turi turėti kibernetinio saugumo ekspertinių žinių bent vienoje iš Reglamente išvardytų sričių. Be to, NKC, atlikdamas subjektų vertinimą, taip pat atsižvelgia į bet kokį aktualų nacionalinių kompetentingų institucijų saugumo tikslais atliktą nacionalinį vertinimą (Reglamento 8 str. 4 d.). Taip pat registracija bet kuriuo metu gali būti atšaukta dėl tam tikrų pagrįstų saugumo priežasčių. Atsižvelgiant į tai, KSĮ projekto 23 straipsnyje siūloma sudaryti galimybę NKC užduotis vykdančiai institucijai kreiptis į institucijas, nurodytas Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo 12 straipsnio 7 dalyje, kurios, vadovaudamosi Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme nurodytais investuotojų

patikros dėl atitikties nacionalinio saugumo interesams vertinimo kriterijais, galėtų įvertinti, ar subjektai, potencialūs bendruomenės nariai, nekelia grėsmės nacionalinio saugumo interesams.

Atsižvelgiant į tai, kad Reglamentas susijęs su kibernetinio saugumo srities inovacijų skatinimu, modelis buvo pasirinktas atsižvelgiant į gerąją praktiką, kuri nustatyta Lietuvos Respublikos krašto apsaugos sistemos organizavimo ir karo tarnybos įstatymo 9 straipsnio 4 dalies 10 punkte. Pagal minėtą įstatymo nuostatą Krašto apsaugos ministerija turi teisę finansuoti eksperimentinę plėtrą ir inovacinę veiklą gynybos ir saugumo srityje Lietuvos Respublikos technologijų ir inovacijų įstatymo ir Lietuvos Respublikos nacionalinių plėtros įstaigų įstatymo nustatyta tvarka. Krašto apsaugos ministerija nefinansuoja eksperimentinės plėtros ar inovacinės veiklos, jeigu tai prieštarauja nacionalinio saugumo interesams. Institucijos, nurodytos Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo 12 straipsnio 7 dalyje, jau vykdo tokią patikrą nuo 2021 m. liepos 1 d., todėl pats procesas šioms institucijoms yra žinomas ir yra susiformavusi tokios veiklos praktika. Atsižvelgiant į tai, kad numatomas Lietuvos kibernetinio saugumo kompetencijos bendruomenės narių skaičius nebūtų itin didelis (apie 170) ir jų registracijos procesas intensyviausias būtų tik įsigaliojus atitinkamam KSĮ projekto straipsniui, sukuriama administracinė našta šioms institucijoms neturėtų būti itin didelė.

KSĮ projekto 23 straipsnio 5 dalyje siūloma nustatyti sąlygas, kokiais atvejais NKC išbraukia Kibernetinio saugumo kompetencijos bendruomenės narį iš bendruomenės, susijusias su reikalavimų, taikomų bendruomenės nariams, neatitikimu ar savanorišku pasitraukimu iš bendruomenės.

15. Siekiant užtikrinti domenų vardų sistemos saugumą, stabilumą ir atsparumą, būtina turėti tikslias ir išsamias domenų vardų registracijos duomenų bazes ir suteikti teisėtą prieigą prie tokių duomenų, o tai savo ruožtu prisidėtų prie aukšto bendro kibernetinio saugumo lygio Lietuvos Respublikoje ir visoje ES. Šiuo konkrečiu tikslu TIS 2 direktyvoje reikalaujama, kad aukščiausio lygio domenų vardų registro paslaugas ir domenų vardų registravimo paslaugas teikiantys subjektai tvarkytų tam tikrus duomenis, būtinus tam tikslui pasiekti. Aukščiausio lygio domenų vardų registro paslaugas ir domenų vardų registravimo paslaugas teikiantys subjektai turėtų bendradarbiauti tarpusavyje, kad būtų išvengta tos užduoties dubliavimosi, todėl siekiant įgyvendinti TIS 2 direktyvos 28 straipsnyje nustatytus reikalavimus aukščiausio lygio domenų vardų registravimo ir domenų vardų registravimo paslaugoms, siūloma KSĮ projekto 17 straipsnyje nustatyti TIS 2 direktyvos 28 straipsnio reikalavimus.

16. Atsižvelgus į tai, kad TIS 2 direktyvos reikalavimai turi būti taikomi ir viešojo administravimo subjektams, kurie laikomi esminiais subjektais, būtina tikslinti galiojančias valstybės informacinių išteklių saugos nuostatas, kad atitiktų TIS 2 direktyvos reikalavimus. Taip pat siekiant bendro kibernetinio saugumo reguliavimo, siūloma KSĮ projektu atsisakyti valstybės informacinių išteklių saugos užtikrinimo nuostatų ir jas integruoti į nuoseklią kibernetinio saugumo subjektams taikomų reikalavimų sistemą. Pirmiausia KSĮ projektu siūloma nustatyti, kad asmuo, kuris Valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka valdo ir (ar) tvarko ypatingos svarbos ir (ar) svarbius valstybės informacinius išteklius, būtų registruojamas kaip esminis subjektas, o asmuo, kuris valdo ir (ar) tvarko mažesnės svarbos kitus valstybės informacinius išteklius, būtų registruojamas kaip svarbus subjektus. Visi kartu šie subjektai (kibernetinio saugumo subjektai) privalės užtikrinti valdomų ir (ar) tvarkomų tinklų ir informacinių sistemų atitiktį kibernetinio saugumo rizikos valdymo priemonėms, tvirtinamoms Vyriausybės, pranešti NKSC apie kibernetinius incidentus ir įgyvendinti kitas kibernetinio saugumo subjektams KSĮ projekte nustatytas pareigas.

KSĮ 22 straipsnyje apibrėžtas saugos įgaliotinio funkcijas siūloma išlaikyti ir taikyti asmenims, atsakingiems už kibernetinį saugumą (KSĮ projekto 15 straipsnis). Atsižvelgus į privačiajame sektoriuje plačiai taikomą praktiką už kibernetinį saugumą skirti vyriausiąjį informacijos saugumo vadovą (angl. CISO) ar kitą informacijos saugumo specialistą, turintį tarptautiniu mastu pripažįstamą sertifikatą informacijos ar kibernetinio saugumo srityje, atitinkamai siūloma KSĮ projekte nustatyti reikalavimą asmenims, atsakingiems už kibernetinį saugumą, turėti patirties šioje srityje. Už kibernetinį saugumą atsakingų asmenų pareigos, kaip nustatyta KSĮ projekto 14 straipsnio 5 dalies 2 punkte, būtų nustatytos kibernetinio saugumo rizikos valdymo priemonėse, tvirtinamose Vyriausybės.

17. KSĮ projektas taip pat tikslinamas dėl naujų nuostatų, kurios nesusijusios su TIS 2 direktyvos perkėlimu.

Siekiant prisidėti prie bendro ES diplomatinio atsako į kibernetines atakas, ypač vertinant, kokių bendros užsienio ir saugumo politikos priemonių, įskaitant atsakomąsias priemones, galima imtis siekiant sustiprinti ES atsaką į veiklą, kuria kenkiama ES politiniams, saugumo ir ekonominiams interesams, pirmiausia būtina stiprinti ir Lietuvos Respublikos gebėjimus priskirti kibernetinę kenkimo veiklą atitinkamiems subjektams, ir politinį atsaką, siekiant daryti įtaką potencialių agresorių elgesiui, taip pat užtikrinti, kad atsakas būtų proporcingas. Šiuo metu ES veikia Kibernetinio saugumo diplomatijos priemonių rinkinys[1], tačiau siekiant reaguoti į didelio masto kibernetinius incidentus Lietuvos Respublikoje būtina daryti pažangą šioje srityje, todėl siūloma KSĮ projekte numatyti Lietuvos Respublikos užsienio reikalų ministerijai dalyvauti formuojant kibernetinio saugumo politiką, nustatant teisinį diplomatinių priemonių taikymo reguliavimą reaguojant į kibernetines grėsmes ir kibernetinius incidentus.

Policijos įgaliojimai kibernetinio saugumo srityje KSĮ projekto 10 straipsnyje išlaikomi iš esmės nepakitę – praktika yra pakankamai nusistovėjusi, policija šiuos įgaliojimus įgyvendina bendrosios kompetencijos teismuose. KSĮ projekto 10 straipsnio 1 dalies 3 punkte nurodytais atvejais, Policija į teismą kreipiasi Civilinio proceso kodekso nustatyta tvarka. Nurodymai yra susiję su paslaugų teikimo apribojimu, be to, orientuoti į nusikalstamų veikų užkardymą ir žalos sumažinimą, todėl administracinis ar baudžiamasis procesai dar nebūna pradedami. Atkreiptinas dėmesys, kad KSĮ projekto 10 straipsnio 1 dalies 3 punkte nustatyta nuostata dėl viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų, elektroninių prekyviečių, interneto paieškos sistemų, debesijos kompiuterijos paslaugų teikimo apribojimo 48 valandoms perkeliama iš galiojančio KSĮ. Siekiant sumažinti galimą kenkimo programinės įrangos žalą, būtina kuo skubiau užkirsti kelią jos plitimui. Pagrindinė nuostata, kad paslaugų teikimas turi būti ribojamas tik teismo sprendimu, tačiau teismo sankcijos gavimas užtrunka ir skubos atvejais ne visada galima tokią sankciją greitai gauti. Siekdama išvengti didesnės žalos ir užfiksuoti tyrimui reikalingus duomenis, policija duoda nurodymą dėl paslaugų teikimo ribojimo, o teismui pateikia teikimą dėl veiksmų pagrįstumo patvirtinimo. KSĮ projekto 10 straipsnio 2 dalis papildoma nuostatomis dėl policijos nurodymo įvykdymo termino. Atsižvelgiant į Reglamento (ES) 2021/784 3 straipsnį, nurodantį, kad prieglobos paslaugų teikėjai pašalina teroristinį turinį ar visose valstybėse narėse panaikina prieigą prie jo kaip įmanoma greičiau ir bet kuriuo atveju per vieną valandą nuo nurodymo pašalinti turinį gavimo, KSĮ projekto 10 straipsnio 2 dalis papildoma nauju nurodymo įvykdymo terminu. Pažymėtina, kad KSĮ projekto 10 straipsnio 2 dalyje nustatyti skubos atvejai apima ne tik teroristinį turinį, nurodymai gali būti duodami atsižvelgiant į nusikalstamų veikų daromą žalą. Įvairių formų nusikaltimai elektroninėje erdvėje kelia vis didesnę grėsmę. Kibernetinės atakos, seksualinis vaikų išnaudojimas internete ir sukčiavimas internete yra labai sudėtingi nusikaltimai ir pasireiškia įvairiomis formomis. Grėsmę keliančių subjektų naudojama taktika, metodai ir procedūros nuolat vystosi, tačiau aiškūs tokių išpuolių motyvai beveik nekinta: vertingos konfidencialios informacijos vagystės, pinigų pritraukimas, manipuliavimas viešąja nuomone ar kenkimas skaitmeninei infrastruktūrai. Jų kibernetinių išpuolių vykdymo tempas vis didėja, o jų kampanijos tampa vis sudėtingesnės, automatizuotos, išpuolių perimetras plečiasi, išnaudojamos tinklų ir informacinių sistemų spragos. Grėsmę keliantys subjektai ir toliau demonstruoja didelį gebėjimą prisitaikyti prie naujų technologijų ir visuomenės raidos, nuolat stiprindami tarpusavio ryšius ir specializaciją. Kibernetines atakas sunku ištirti, nes jas sudaro keli žingsniai nuo pradinio įsibrovimo, jungiantis per šifruotas ir anonimines prieigas, iki duomenų gavimo ir panaudojimo. Policijos nurodymai dėl paslaugų teikimo jų gavėjui apribojimo ar (ir) nurodymai paslaugų teikėjams išsaugoti su jų teikiamomis paslaugomis susijusią informaciją dažniausiai susiję su išpirkos reikalaujančia kenkimo programine įranga (angl. *ransomware*), siekiant užkirsti kelią kenkimo programinės įrangos plitimui ar (ir) išsaugoti tyrimui reikalingus duomenis, taip pat tokio pobūdžio nurodymai aktualūs įvykus įsibrovimui į informacines sistemas, duomenų nutekinimui, vykstant paskirstytos paslaugos

[1] https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf

trikdymo atakoms prieš Lietuvos Respublikos infrastruktūrą. Delsimas taikyti atitinkamas priemones gali lemti žalos dydį ir nusikalstamos veikos mastą, svarbių duomenų praradimą.

Be esminių pakeitimų išlaikomos KSĮ 9 straipsnio (Valstybinės duomenų apsaugos inspekcijos įgaliojimai kibernetinio saugumo srityje), VI skyriaus (Nacionalinės kibernetinio saugumo sertifikavimo institucijos įgaliojimai), 25 straipsnio (Saugusis tinklas), 26 straipsnio (Duomenų centrų naudojimas) nuostatos.

18. Siekiant užtikrinti sklandų naujos redakcijos KSĮ įsigaliojimą, nustatomos pereinamojo pobūdžio nuostatos pakeitimo įstatymo 2 straipsnyje:

3 dalyje numatoma NKSC pareiga iki 2025 m. balandžio 17 d. identifikuoti KSĮ 1 ir 2 prieduose nurodytuose sektoriuose veikiančius kibernetinio saugumo subjektus ir juos įtraukti į Kibernetinio saugumo subjektų registrą – taip įgyvendinama pareiga, numatyta TIS 2 direktyvos 3 straipsnio 5 dalyje.

Atsižvelgiant į šiuo metu identifikuotų ypatingos svarbos informacinės infrastruktūros valdytojų svarbą, 4 dalyje numatoma pareiga ypatingos svarbos informacinės infrastruktūros valdytojams toliau užtikrinti šiuo metu galiojančius kibernetinio saugumo reikalavimus tol, kol bus sudarytas naujas Kibernetinio saugumo subjektų registras (iki 2025 m. balandžio 17 d.). Ypatingos svarbos informacinės infrastruktūros valdytojai, kurie nebūtų identifikuoti kaip kibernetinio saugumo subjektai, turėtų teisę netaikyti kibernetinio saugumo reikalavimų. Pažymėtina, kad tai yra labiau teorinio pobūdžio teisė, nes numatoma, kad visi ypatingos svarbos informacinės infrastruktūros valdytojai bus įtraukti į Kibernetinio saugumo subjektų registrą.

Atsižvelgiant į tai, nuo registracijos Kibernetinio saugumo subjektų registre tik bus pradėtas skaičiuoti 14 straipsnio 2 dalyje nurodytas kibernetinio saugumo rizikos valdymo priemonių įgyvendinimo terminas, kuris numatomas ne mažesnis nei 12 mėn. Atsižvelgiant į tai, kad negalima sukurti tokios situacijos, kai ypatingos svarbos informacinės infrastruktūros valdytojams netaikomos jokios kibernetinio saugumo rizikos valdymo priemones, 5 dalyje nustatoma iš esmės analogiška kaip ir 4 dalyje pareiga atitikti iki įstatymo įsigaliojimo galiojusius reikalavimus tol, kol Vyriausybės nustatyta tvarka pradės galioti kiti reikalavimai.

6 dalyje numatomos pereinamojo pobūdžio priemonės saugos įgaliotiniams. Esminė taisyklė – nustatomas 2 metų terminas atitikti naujos redakcijos KSĮ 15 straipsnio 5 dalies 3 punkte nustatytus reikalavimus.

7 ir 8 dalyse numatoma, kad NKSC 4 ir 5 dalyje numatytais atvejais priežiūrą atliktų iki šio įstatymo įsigaliojimo galiojusia tvarka. Pažymėtina, kad naujos redakcijos KSĮ numatoma daugiau ir veiksmingesni NKSC įgaliojimai atliekant kibernetinio saugumo subjektų priežiūrą. Atsižvelgiant į tai ir siekiant nebloginti ypatingos svarbos informacinės infrastruktūros valdytojų padėties, iki naujos redakcijos įstatymo įsigaliojimo galiojusių reikalavimų priežiūrą numatoma atlikti iki šio įstatymo įsigaliojimo galiojusia tvarka.

9 dalyje numatoma, kad iki įstatymo įsigaliojimo pradėtos procedūros tęsiamos ir baigiamos vadovaujantis iki įstatymo įsigaliojimo galiojusiomis nuostatomis.

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

Kartu su Įstatymų projektais yra teikiamas atskiras dokumentas – numatomo teisinio reguliavimo poveikio vertinimo pažyma.

6. Kokią įtaką priimti įstatymai turės kriminogeninei situacijai, korupcijai

KSĮ projektas neturės įtakos kriminogeninei situacijai ir korupcijai.

7. Kaip įstatymų įgyvendinimas atsilieps verslo sąlygoms ir jo plėtrai

Įstatymo projekto įgyvendinimas ilguoju laikotarpiu teigiamai atsilieps verslo sąlygoms ir jo

plėtrai, kadangi KSĮ projekto įgyvendinimas turės įtakos kuriant saugesnę kibernetinę erdvę paslaugoms teikti Lietuvos Respublikoje.

Sustiprinti kibernetinio saugumo pajėgumai organizacijose galėtų daryti įtaką ir paskatinti šias organizacijas naudoti naujausios kartos informacinių ir ryšių tinklų infrastruktūrą ir paslaugas, kurios taip pat būtų ekologiškesnės, pakeistų neefektyvią ir mažiau saugią pasenusią įrangą. Tikimasi, kad KSĮ projektas padės sumažinti kibernetinių incidentų skaičių ir jų poveikį bei atitinkamai atlaisvins organizacijų finansinius išteklius tvarioms investicijoms.

8. Įstatymo projekto atitiktis strateginio lygmens planavimo dokumentams

KSĮ projektas neprieštarauja strateginio lygmens planavimo dokumentams ir prisideda prie Aštuonioliktosios Lietuvos Respublikos Vyriausybės programos 238.1 papunktyje nurodyto siekio stiprinti nacionalinius kibernetinio saugumo pajėgumus ir valstybės informacinių išteklių, kritinės infrastruktūros kibernetinę apsaugą, taip pat užtikrina kibernetinio saugumo funkcijų konsolidavimą.

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

Siekiant KSĮ projekte siūlomus pakeitimus įtraukti į teisinę sistemą, reikės priimti, pakeisti ir pripažinti netekusiais galios aiškinamojo rašto 12 punkte nurodytus teisės aktus.

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

KSĮ projektas parengtas laikantis Lietuvos Respublikos valstybinės kalbos įstatymo, Lietuvos Respublikos teisėkūros pagrindų įstatymo reikalavimų. KSĮ projektu apibrėžiamos sąvokos ir juos įvardijantys terminai vertinami Lietuvos Respublikos terminų banko įstatymo nustatyta tvarka.

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

KSĮ projektas atitinka Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos nuostatas ir ES dokumentus.

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

12.1. Priėmus KSĮ projektą, Vyriausybė iki 2024 m. spalio 17 d. turės priimti šiuos teisės aktus:

12.1.1. Kibernetinio saugumo subjektų identifikavimo pagal specialiuosius kriterijus metodiką (rengėja – Krašto apsaugos ministerija);

12.1.2. Kibernetinio saugumo įstatymo 1 ir 2 prieduose nurodytiems sektoriams taikomų ES teisės aktų (jeigu yra), kurių poveikis yra lygiavertis Kibernetinio saugumo įstatymo reikalavimams, sąrašą (rengėjos – sektoriuose politiką formuojančios ministerijos);

12.1.3. Vykdymo užtikrinimo priemonių taikymo esminiams ir svarbiems subjektams tvarkos aprašą (rengėja – Krašto apsaugos ministerija).

12.2. Priėmus KSĮ projektą, Vyriausybė iki 2024 m. spalio 17 d. turės pakeisti Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimą Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (rengėja – Krašto apsaugos ministerija):

12.2.1. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašą (rengėja – Krašto apsaugos ministerija);

12.2.2. Nacionalinį kibernetinių incidentų valdymo planą (rengėja – Krašto apsaugos ministerija);

12.2.3. Nacionalinę kibernetinio saugumo strategiją (rengėja – Krašto apsaugos ministerija);

12.2.4. Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką (rengėja – Krašto apsaugos ministerija).

12.3. Priėmus KSĮ projektą, Krašto apsaugos ministerija iki 2024 m. spalio 17 d. turės pakeisti šiuos teisės aktus:

12.3.1. Lietuvos Respublikos krašto apsaugos ministro 2021 m. rugpjūčio 9 d. įsakymą Nr. V-484 „Dėl Nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašo patvirtinimo“;

12.3.2. Lietuvos Respublikos krašto apsaugos ministro 2019 m. lapkričio 27 d. įsakymą Nr. V-998 „Dėl Kibernetinio saugumo informacinio tinklo nuostatų patvirtinimo“;

12.3.3. Lietuvos Respublikos krašto apsaugos ministro 2017 m. rugpjūčio 31 d. įsakymą Nr. V-804 „Dėl Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatų ir struktūros patvirtinimo“;

12.3.4. Lietuvos Respublikos krašto apsaugos ministro 2015 m. gegužės 5 d. įsakymą Nr. V-461 „Dėl Techninių kibernetinio saugumo priemonių diegimo ir valdymo valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėje infrastruktūroje tvarkos aprašo patvirtinimo“;

12.3.5. Lietuvos Respublikos krašto apsaugos ministro 2015 m. gegužės 26 d. įsakymą Nr. V-535 „Dėl Kibernetinio saugumo tarybos reglamento ir personalinės sudėties patvirtinimo“;

12.3.6. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymą Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“.

12.4. Priėmus KSĮ projektą, Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos iki 2024 m. spalio 17 d. turės priimti:

12.4.1. Mokymų tvarkos aprašą kibernetinio saugumo subjektų vadovams, už kibernetinį saugumą atsakingiems asmenims, kibernetinio saugumo auditą atliekantiems asmenims;

12.4.2. Kibernetinio saugumo auditų atlikimo metodiką.

12.5. Priėmus KSĮ projektą ir patvirtinus susijusius teisės aktus, iki 2024 m. spalio 17 d. reikės pripažinti netekusiu galios Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimą Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“ (rengėja – Krašto apsaugos ministerija).

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)

Kartu su Įstatymų projektais yra teikiamas atskiras dokumentas – numatomo teisinio reguliavimo poveikio vertinimo pažyma, kurioje pateikti skaičiavimai, kiek valstybės, savivaldybių biudžetų lėšų prireiks Įstatymams įgyvendinti.

14. Įstatymų projektų rengimo metu gauti specialistų vertinimai ir išvados

Įstatymo projekto rengimo metu gautos išvados suderintos darbo tvarka.

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

Kibernetinis saugumas, kibernetinis incidentas, kibernetinio saugumo rizikos valdymo priemonės, TIS 2 direktyva, esminis subjektas, svarbus subjektas.

16. Kiti, iniciatorių nuomone, reikalingi pagrindimai ir paaiškinimai

Nėra.

_____