2016 M. LIEPOS 6 D. EUROPOS PARLAMENTO IR TARYBOS DIREKTYVOS (ES) 2016/1148 DĖL PRIEMONIŲ AUKŠTAM BENDRAM TINKLŲ IR INFORMACINIŲ SISTEMŲ SAUGUMO LYGIUI VISOJE SĄJUNGOJE UŽTIKRINTI 7 STRAIPSNIO IR NACIONALINIŲ TEISĖS AKTŲ ATITIKTIES LENTELĖ

Direktyvos (kito Europos Sąjungos (ES) teisės akto) pavadinimas ir numeris	**Lietuvos Respublikos nacionalinio teisės akto (teisės akto projekto) pavadinimas**	**Direktyvos (kito ES teisės akto) perkėlimo (įgyvendinimo) lygis (visiškas, dalinis)**
2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (toliau – Direktyva)	**1. Lietuvos Respublikos Vyriausybės nutarimo projektas „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ (toliau – Strategijos projektas).** **2. Lietuvos Respublikos kibernetinio saugumo įstatymas Nr. XII-1428 (toliau – Kibernetinio saugumo įstatymas)**	
7 straipsnis. Nacionalinė tinklų ir informacinių sistemų saugumo strategija 1. Kiekviena valstybė narė priima nacionalinę tinklų ir informacinių sistemų saugumo strategiją, kurioje apibrėžiami strateginiai tikslai ir tinkamos politikos bei reguliavimo priemonės aukšto lygio tinklų ir informacinių sistemų saugumui pasiekti ir išlaikyti, ir kuri apima bent II priede nurodytus sektorius ir III priede nurodytas paslaugas. Nacionalinėje tinklų ir informacinių sistemų saugumo strategijoje visų pirma nagrinėjami šie klausimai:	**1. Kibernetinio saugumo įstatymas** **1 straipsnis. Įstatymo paskirtis ir taikymas** 1. Šis įstatymas nustato kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigas, taip pat tarpinstitucinį bendradarbiavimą. <...> **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> 8. **Kibernetinio saugumo subjektas** – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių	Visiškas

	tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas. <...> **5 straipsnis. Vyriausybės įgaliojimai kibernetinio saugumo srityje** Vyriausybė: 1) tvirtina Nacionalinę kibernetinio saugumo strategiją; <...> **2. Strategijos projektas**	
a) nacionalinės tinklų ir informacinių sistemų saugumo strategijos tikslai ir prioritetai;	**1. Kibernetinio saugumo įstatymas** **4 straipsnis. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos** 1. Kibernetinio saugumo politikos strateginius tikslus, prioritetus ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė. <...> **2. Strategijos projektas** 1. Nacionalinė kibernetinio saugumo strategija (toliau – Strategija) nustato svarbiausias nacionalinės kibernetinio saugumo politikos viešajame ir privačiame sektoriuose kryptis. Įgyvendinant Strategiją siekiama stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą, užtikrinti nusikalstamų veikų, kurias vykdant naudojami kibernetinę erdvę sudarantys objektai (toliau – nusikalstamos veikos kibernetinėje erdvėje), prevenciją, užkardymą ir tyrimą, skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą, stiprinti glaudų viešojo ir privataus sektorių, tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą valstybėje iki 2023 m.	Visiškas

	<...> 4. Strategijos pagrindinis tikslas – efektyviai ir laiku identifikuojant kibernetinius incidentus, užkertant kelią jų atsiradimui ir plitimui, valdant kibernetinių incidentų sukeltas pasekmes, užtikrinti galimybę Lietuvos visuomenei saugiai naudotis informacinių ir ryšių technologijų (toliau – IRT) teikiamomis galimybėmis. 5. **Pirmasis Strategijos tikslas** – stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą. <...> 15. **Antrasis Strategijos tikslas** – užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą. <...> 23. **Trečiasis Strategijos tikslas** – skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą. <...> 33. **Ketvirtasis Strategijos tikslas** – stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą. <...> 39. **Penktasis Strategijos tikslas** – stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą.	
b) valdymo sistema, skirta nacionalinės tinklų ir informacinių sistemų saugumo strategijos tikslams ir prioritetams įgyvendinti, įskaitant valdžios įstaigų ir kitų atitinkamų subjektų vaidmenis ir įsipareigojimus;	**1. Kibernetinio saugumo įstatymas** **4 straipsnis. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos** <...> 2. Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija. Nacionalinis kibernetinio saugumo	Visiškas

	centras formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek šiame įstatyme nustatytoms funkcijoms atlikti reikia nustatyti kibernetinio saugumo subjektų veiklos teisinį reguliavimą. 3. Kibernetinio saugumo politiką įgyvendina Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija, Lietuvos policija ir kitos institucijos, kurių funkcijos yra susijusios su kibernetiniu saugumu. **2. Strategijos projektas** <...> 43. Siekdama įgyvendinti Strategijos tikslus ir uždavinius, Lietuvos Respublikos Vyriausybė tvirtina tarpinstitucinį veiklos planą, kuriame nustatomos Strategijos įgyvendinimo priemonės ir lėšos joms įgyvendinti. Šio plano rengimą koordinuoja Krašto apsaugos ministerija, dalyvaujant NKSC. Įgyvendinant Strategiją, pagal savo kompetenciją dalyvauja ministerijos, kitos valstybės ir (ar) savivaldybių institucijos, įstaigos ir (ar) organizacijos, nurodytos Strategijos tarpinstituciniame veiklos plane (toliau – Strategijos vykdytojai). 44. Nevyriausybinės organizacijos, suinteresuoti kiti viešojo ir privataus sektoriaus atstovai, Lietuvos mokslo ir studijų institucijos gali prisidėti prie Strategijos vykdymo, jos tikslų ir uždavinių siekimo.	
c) parengties, reagavimo ir atkūrimo priemonių, įskaitant viešojo ir privačiojo sektorių bendradarbiavimą, nustatymas;	**Strategijos projektas** <...> 5. **Pirmasis Strategijos tikslas** – stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą. <...> 14. **Uždaviniai pirmajam Strategijos tikslui pasiekti:** 14.1. *Pirmasis pirmojo tikslo uždavinys* – kurti sisteminį požiūrį į	Visiškas

	kibernetinį saugumą ir prevencinę veiklą. Šis uždavinys bus įgyvendinamas tobulinant kibernetinio saugumo rizikos nustatymo, vertinimo ir prognozavimo būdus, formuojant kibernetinio saugumo atpažinties paveikslą ir rizikos žemėlapį, kuris atskleistų atskiriems sektoriams būdingas rizikas, kuriant regioninį kibernetinio saugumo centrą ir valstybės valdomą elektroninių ryšių tinklą su kompleksinėmis kibernetinio saugumo priemonėmis, jungiantį valstybines mobilizacines užduotis gyvybiškai svarbioms valstybės funkcijoms atlikti paskirtas vykdyti valstybės ir savivaldybių institucijas, įstaigas ir įmones, atliekant kibernetinio saugumo būsenos tyrimus, pažangos matavimus ar brandos vertinimus, užtikrinant visuomenės informavimą apie kibernetinio saugumo būklę, vykdant kitas kibernetinį saugumą ir prevencinę veiklą stiprinančias priemones ir veiksmus. 14.2. *Antrasis pirmojo tikslo uždavinys* – didinti kibernetinio saugumo politikos formavimo ir įgyvendinimo efektyvumą, mažinant administracinę naštą kibernetinio saugumo subjektams. Šis uždavinys bus įgyvendinamas tobulinant kibernetinio saugumo teisinį reguliavimą, parengiant standartizuotus, bet diferencijuojamus kibernetinio saugumo reikalavimus, atliekant gerosios praktikos, standartų, taikomų užtikrinant kibernetinį saugumą, analizę, skatinant kibernetinio saugumo subjektus jais vadovautis, nustatant nacionalinį integruotą krizių valdymo mechanizmą, užtikrinant visų lygmenų struktūrų sklandų bendradarbiavimą, atnaujinant kibernetinio saugumo rizikos vertinimo sistemą, įvertinant metodines galimybes vykdyti kibernetiniam saugumui reikalingų lėšų stebėseną ir kontrolę, nustatant jų skyrimo ir naudojimo pirmumą, vykdant kitas kibernetinio saugumo politikos formavimo ir įgyvendinimo plėtojimo priemones. 14.3. *Trečiasis pirmojo tikslo uždavinys* – skatinti nacionalinių	

	pratybų vykdymą ir dalyvavimą tarptautinėse pratybose. Šis uždavinys bus įgyvendinamas periodiškai rengiant kompleksines nacionalines kibernetinio saugumo pratybas, dalyvaujant Europos Sąjungos, NATO ir kitų šalių organizuojamose pratybose, integruojant nacionalinių ir tarptautinių pratybų patirtį atliekant situacijų valdymo, incidentų vertinimo, informacijos komunikavimo ar kitus veiksmus. 14.4. *Ketvirtasis pirmojo tikslo uždavinys* – plėtoti valstybės kibernetinės gynybos pajėgumus. Šis uždavinys bus įgyvendinamas užtikrinant efektyvią Lietuvos kariuomenės sąveiką su valstybės civiliniais pajėgumais, plėtojant kibernetinės gynybos pajėgumus ir teikiant pagalbą kitoms valstybės ir savivaldybių institucijoms ir įstaigoms. <...> 33. **Ketvirtasis Strategijos tikslas** – stiprinti glaudų privataus ir viešojo sektorių bendradarbiavimą. <...> 38. **Uždaviniai ketvirtajam Strategijos tikslui pasiekti:** 38.1. *Pirmasis ketvirtojo tikslo uždavinys* – gerinti viešojo ir privataus sektorių bendradarbiavimo koordinavimą. Šis uždavinys bus įgyvendinamas kuriant tvarų privataus ir viešojo sektoriaus bendradarbiavimo kibernetinio saugumo srityje modelį, nustatant atsakomybę ir pajėgumus didinant valstybės kibernetinį atsparumą, efektyvinant viešojo ir privataus sektorių atstovų keitimąsi aktualia informacija apie kibernetines grėsmes, įvykusius kibernetinius incidentus, išmoktas pamokas, plėtojant ankstyvojo perspėjimo sistemą ir abipusio keitimosi informacija apie kibernetines grėsmes mechanizmus, kuriant naujus arba tobulinant esamus komunikacijos metodus ir procesus, didinant kibernetinio saugumo informacijos mainų platformos veiklos efektyvumą. 38.2. *Antrasis ketvirtojo tikslo uždavinys* – didinti mažų ir	

	vidutinių viešojo ir privataus sektorių atstovų kibernetinio saugumo brandą. Šis uždavinys bus įgyvendinamas skatinant mažas ir vidutines viešojo ir privataus sektoriaus įmones tikrintis kibernetinio saugumo būklę, taisyti kibernetinio saugumo spragas. 38.3. *Trečiasis ketvirtojo tikslo uždavinys* – kurti atsakingą viešojo ir privataus sektorių IRT saugumo spragų atskleidimo praktiką. Šis uždavinys bus įgyvendinamas inicijuojant atsakingą viešojo ir privataus sektorių IRTspragų atskleidimo praktiką, nustatant šios srities veiklos principus, metodų, techninių gebėjimų ar kitų priemonių taikymo tvarką.	
d) švietimo, informuotumo didinimo ir mokymo programų, susijusių su nacionaline tinklų ir informacinių sistemų saugumo strategija, nurodymas;	**Strategijos projektas** <...> 23. **Trečiasis Strategijos tikslas –** skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą. <...> 32. **Uždaviniai trečiajam Strategijos tikslui pasiekti:** 32.1. *Pirmasis trečiojo tikslo uždavinys* – plėtoti mokslinius tyrimus ir didelę pridėtinę vertę kuriančias veiklas kibernetinio saugumo srityje. Šis uždavinys bus įgyvendinamas sudarant palankias sąlygas kurti naujas, pažangius gebėjimus plėtojančias kibernetinio saugumo iniciatyvas, skatinant kibernetinio saugumo rinkos augimą, kibernetinio saugumo paslaugų eksportą į užsienio rinkas, plėtojant finansinių technologijų kibernetinio saugumo sektorių ir atliekant mokslinius tyrimus. 32.2. *Antrasis trečiojo tikslo uždavinys* – ugdyti kūrybiškumą, pažangius gebėjimus ir rinkos poreikius atitinkančius kibernetinio saugumo įgūdžius ir kvalifikaciją. Šis uždavinys bus įgyvendinamas verslui, akademinei bendruomenei ir valstybei kuriant kibernetinio saugumo kompetencijų modelį, formuojant kibernetinio saugumo kompetencijų standartus, plėtojant šios	Visiškas

	srities mokymų, akreditavimo ir sertifikavimo sistemas, orientuotas į darbo rinkos poreikius, pritraukiant ir ugdant talentus, kuriant kibernetinio saugumo mokymų ir testavimo aplinką, mokant naujokus ir sudarant persikvalifikavimo galimybes informacinių technologijų srityje dirbantiems asmenims, tobulinant asmenų, dirbančių su jautriais duomenimis, kibernetinio saugumo žinias. 32.3. *Trečiasis trečiojo tikslo uždavinys* – skatinti viešojo ir privataus sektorių ir mokslo bendradarbiavimą, kuriant kibernetinio saugumo srities inovacijas. Šis uždavinys bus įgyvendinamas nustatant bendrus viešojo ir privataus sektorių poreikius ir jų svarbą moksliniams kibernetinio saugumo tyrimams, skatinant mokslo, viešojo ir privataus sektorių bendradarbiavimą, kuriant technines priemones, metodus ar kitus išteklius, ugdant gebėjimus išspręsti kibernetinio saugumo problemas ar vykdyti specifines kibernetinio saugumo užduotis.	
e) mokslinių tyrimų ir plėtros planų, susijusių su nacionaline tinklų ir informacinių sistemų saugumo strategija, nurodymas;	**Strategijos projektas** <...> 23. **Trečiasis Strategijos tikslas –** skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą. <...> **32. Uždaviniai trečiajam Strategijos tikslui pasiekti:** 32.1. *Pirmasis trečiojo tikslo uždavinys* – plėtoti mokslinius tyrimus ir didelę pridėtinę vertę kuriančias veiklas kibernetinio saugumo srityje. Šis uždavinys bus įgyvendinamas sudarant palankias sąlygas kurti naujas, pažangius gebėjimus plėtojančias kibernetinio saugumo iniciatyvas, skatinant kibernetinio saugumo rinkos augimą, kibernetinio saugumo paslaugų eksportą į užsienio rinkas, plėtojant finansinių technologijų kibernetinio saugumo sektorių ir atliekant mokslinius tyrimus.	Visiškas

	32.2. *Antrasis trečiojo tikslo uždavinys* – ugdyti kūrybiškumą, pažangius gebėjimus ir rinkos poreikius atitinkančius kibernetinio saugumo įgūdžius ir kvalifikaciją. Šis uždavinys bus įgyvendinamas verslui, akademinei bendruomenei ir valstybei kuriant kibernetinio saugumo kompetencijų modelį, formuojant kibernetinio saugumo kompetencijų standartus, plėtojant šios srities mokymų, akreditavimo ir sertifikavimo sistemas, orientuotas į darbo rinkos poreikius, pritraukiant ir ugdant talentus, kuriant kibernetinio saugumo mokymų ir testavimo aplinką, mokant naujokus ir sudarant persikvalifikavimo galimybes informacinių technologijų srityje dirbantiems asmenims, tobulinant asmenų, dirbančių su jautriais duomenimis, kibernetinio saugumo žinias. 32.3. *Trečiasis trečiojo tikslo uždavinys* – skatinti viešojo ir privataus sektorių ir mokslo bendradarbiavimą, kuriant kibernetinio saugumo srities inovacijas. Šis uždavinys bus įgyvendinamas nustatant bendrus viešojo ir privataus sektorių poreikius ir jų svarbą moksliniams kibernetinio saugumo tyrimams, skatinant mokslo, viešojo ir privataus sektorių bendradarbiavimą, kuriant technines priemones, metodus ar kitus išteklius, ugdant gebėjimus išspręsti kibernetinio saugumo problemas ar vykdyti specifines kibernetinio saugumo užduotis.	
f) rizikos vertinimo planas, skirtas rizikai nustatyti;	**1. Kibernetinio saugumo įstatymas** <...> **3 straipsnis. Kibernetinio saugumo principai** 1. Kibernetinis saugumas grindžiamas šiais kibernetinio saugumo principais: <...> 2) **kibernetinio saugumo rizikos valdymo** – taikomos kibernetinio saugumo priemonės turi užtikrinti kibernetinio saugumo subjektų reguliariai įvertinamos rizikos suvaldymą;	Visiškas

	<...> 5. **Pirmasis Strategijos tikslas** – stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą. <...> 14. **Uždaviniai pirmajam Strategijos tikslui pasiekti:** 14.1. *Pirmasis pirmojo tikslo uždavinys* – kurti sisteminį požiūrį į kibernetinį saugumą ir prevencinę veiklą. Šis uždavinys bus įgyvendinamas tobulinant kibernetinio saugumo rizikos nustatymo, vertinimo ir prognozavimo būdus, formuojant kibernetinio saugumo atpažinties paveikslą ir rizikos žemėlapį, kuris atskleistų atskiriems sektoriams būdingas rizikas, kuriant regioninį kibernetinio saugumo centrą ir valstybės valdomą elektroninių ryšių tinklą su kompleksinėmis kibernetinio saugumo priemonėmis, jungiantį valstybines mobilizacines užduotis gyvybiškai svarbioms valstybės funkcijoms atlikti paskirtas vykdyti valstybės ir savivaldybių institucijas, įstaigas ir įmones, atliekant kibernetinio saugumo būsenos tyrimus, pažangos matavimus ar brandos vertinimus, užtikrinant visuomenės informavimą apie kibernetinio saugumo būklę, vykdant kitas kibernetinį saugumą ir prevencinę veiklą stiprinančias priemones ir veiksmus. 14.2. *Antrasis pirmojo tikslo uždavinys* – didinti kibernetinio saugumo politikos formavimo ir įgyvendinimo efektyvumą, mažinant administracinę naštą kibernetinio saugumo subjektams. Šis uždavinys bus įgyvendinamas tobulinant kibernetinio saugumo teisinį reguliavimą, parengiant standartizuotus, bet diferencijuojamus kibernetinio saugumo reikalavimus, atliekant gerosios praktikos, standartų, taikomų užtikrinant kibernetinį saugumą, analizę, skatinant kibernetinio saugumo subjektus jais vadovautis, nustatant nacionalinį integruotą krizių valdymo mechanizmą, užtikrinant visų lygmenų struktūrų sklandų bendradarbiavimą tarpusavyje, atnaujinant kibernetinio saugumo	

	rizikos vertinimo sistemą, įvertinant metodines galimybes vykdyti kibernetiniam saugumui reikalingų lėšų stebėseną ir kontrolę, nustatant jų skyrimo ir naudojimo pirmumą, vykdant kitas kibernetinio saugumo politikos formavimo ir įgyvendinimo plėtojimo priemones. **<...>**	
g) įvairių subjektų, dalyvaujančių įgyvendinant nacionalinę tinklų ir informacinių sistemų saugumo strategiją, sąrašas.	**Strategijos projektas** <...> 43. Siekdama įgyvendinti Strategijos tikslus ir uždavinius, Lietuvos Respublikos Vyriausybė tvirtina tarpinstitucinį veiklos planą, kuriame nustatomos Strategijos įgyvendinimo priemonės ir lėšos joms įgyvendinti. Šio plano rengimą koordinuoja Krašto apsaugos ministerija, dalyvaujant NKSC. Įgyvendinant Strategiją, pagal savo kompetenciją dalyvauja ministerijos, kitos valstybės ir (ar) savivaldybių institucijos, įstaigos ir (ar) organizacijos, nurodytos Strategijos tarpinstituciniame veiklos plane (toliau – Strategijos vykdytojai). 44. Nevyriausybinės organizacijos, suinteresuoti kiti viešojo ir privataus sektoriaus atstovai, Lietuvos mokslo ir studijų institucijos gali prisidėti prie Strategijos vykdymo, jos tikslų ir uždavinių siekimo.	Visiškas
2. Valstybės narės gali prašyti ENISA padėti parengti nacionalines tinklų ir informacinių sistemų saugumo strategijas.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
3. Valstybės narės pateikia Komisijai nacionalines tinklų ir informacinių sistemų saugumo strategijas per tris mėnesius nuo jų priėmimo. Tai darydamos valstybės narės gali nepranešti apie su nacionaliniu saugumu susijusius strategijos elementus.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	

Krašto apsaugos viceministras
Edvinas Kerza

Užsienio reikalų ministras
Linas Linkevičius

Krašto apsaugos viceministras
Vytautas Umbrasas