PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2018-08-10 nutarimu Nr. 12-01-1112

NACIONALINĖ KIBERNETINIO SAUGUMO STRATEGIJA

I SKYRIUS
BENDROSIOS NUOSTATOS

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.

2. Strategija parengta atsižvelgiant į aplinkos analizę, atliktų tyrimų duomenis, viešojo ir privataus sektoriaus atstovų pasiūlymus ir atitinka Septynioliktosios Lietuvos Respublikos Vyriausybės programos, kuriai pritarta Lietuvos Respublikos Seimo 2016 m. gruodžio 13 d. nutarimu Nr. XIII-82 „Dėl Lietuvos Respublikos Vyriausybės programos“, Nacionalinio saugumo strategijos, patvirtintos Lietuvos Respublikos Seimo 2002 m. gegužės 28 d. nutarimu Nr. IX-907 „Dėl Nacionalinio saugumo strategijos patvirtinimo“, Lietuvos Respublikos kibernetinio saugumo įstatymo, Europos Parlamento, Tarybos, Europos Komisijos komunikatų ir rekomendacijų kibernetinio saugumo srityje, taip pat Europos Komisijos 2015 m. gegužės 6 d. komunikato Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui „Europos skaitmeninės rinkos strategija“ ir Informacinės visuomenės plėtros 2014–2020 metų programos „Lietuvos Respublikos skaitmeninė darbotvarkė“, patvirtintos Lietuvos Respublikos Vyriausybės 2014 m. kovo 12 d. nutarimu Nr. 244 „Dėl Informacinės visuomenės plėtros 2014–2020 metų programos „Lietuvos Respublikos skaitmeninė darbotvarkė“ patvirtinimo“ nuostatas. Lietuvai tapus visaverte Europos ekonominio bendradarbiavimo ir plėtros organizacijos nare, šios organizacijos rekomendacijos dėl skaitmeninės rizikos valdymo, ekonominio ir socialinio klestėjimo taip pat yra viena iš svarbių gairių, kuriomis paremta Strategija.

3. Strategijoje vartojamos sąvokos atitinka Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos krašto apsaugos sistemos organizavimo ir karo tarnybos įstatyme, Lietuvos Respublikos mokslo ir studijų įstatyme, Lietuvos Respublikos teisės gauti informaciją iš valstybės ir savivaldybių institucijų ir įstaigų įstatyme apibrėžtas sąvokas.

II SKYRIUS
STRATEGIJOS TIKSLAI, UŽDAVINIAI, VERTINIMO KRITERIJAI IR JŲ REIKŠMĖS

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.

PIRMASIS SKIRSNIS
VALSTYBĖS KIBERNETINIS ATSPARUMAS IR KIBERNETINIAI GYNYBOS PAJĖGUMAI

5. **Pirmasis Strategijos tikslas** – stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą.

6. Lietuva, kaip ir kitos pasaulio valstybės, kuriose aktyviai naudojamasi IRT teikiamomis galimybėmis, turinčios puikiai išplėtotą plačiajuosčio ryšio infrastruktūrą, tampa patraukli ne tik pavieniams asmenims, jų grupuotėms ar organizuotoms grupėms, bet ir Lietuvos Respublikos valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos (toliau – VSD ir AOTD) rengiamose kasmetinėse Grėsmių nacionaliniam saugumui vertinimo ataskaitose įvardytoms valstybėms, keliančioms grėsmę Lietuvos nacionaliniam saugumui ir vykdančioms priešišką veiklą pasaulio ir Lietuvos kibernetinėje erdvėje. Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC), VSD ir AOTD surinkti duomenys rodo, kad Lietuva nuolat susiduria su įvairaus tipo kibernetiniais incidentais, skirtais pažeisti valstybės informacinius išteklius ir ypatingos svarbos informacinę infrastruktūrą, ir prognozuojama, kad ateityje jų skaičius ir mastas nemažės[1].

7. 2017 m. Nacionalinio kibernetinio saugumo būklės ataskaitos duomenimis, 2017 m. Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apdorojo 54 414 kibernetinius incidentus. 2017 m. kibernetinių incidentų užregistruota dešimtadaliu daugiau nei 2016 m. Lietuvos valstybės informaciniai ištekliai tebėra prioritetinis kibernetinio šnipinėjimo taikinys, bet taikomasi ir į privataus sektoriaus ypatingos svarbos informacinę infrastruktūrą, kitas įmones, turinčias strateginę ar svarbią reikšmę nacionaliniam saugumui. NKSC, naudodamas technines kibernetinio saugumo priemones, daugiausiai kenkimo programinės įrangos paplitimo atvejų nustatė energetikos (27 proc.), viešojo saugumo ir teisinės tvarkos (22 proc.) bei užsienio reikalų ir saugumo politikos (21 proc.) sektoriuose. Palyginti su 2016 m., kenkimo programinė įranga labiau plito viešojo saugumo ir teisinės tvarkos, užsienio reikalų ir saugumo politikos, energetikos

[1] Lietuvos Respublikos valstybės saugumo departamentas ir Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos (2018). *Grėsmių nacionaliniam saugumui vertinimas*; Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (2018). *2017 m. Nacionalinio kibernetinio saugumo būklės ataskaita.*

sektoriuose. Šalies kibernetinio saugumo situacijai įtaką daro ir viešojo sektoriaus interneto svetainių būklė, kuri, 2017 m. Nacionalinio kibernetinio saugumo būklės ataskaitos duomenimis, 2017 m. pablogėjo.

8. NKSC, VSD ir AOTD kasmetinėse ataskaitose pateikiama informacija apie kibernetinių incidentų paplitimo mastą rodo, kad kiekvienas kibernetinio saugumo subjektas susiduria su situacija, kai reikia spręsti, kiek laiko, pinigų ar kitų išteklių gali prireikti turimų ryšių ir informacinių sistemų ar teikiamų paslaugų apsaugai. Kibernetinio saugumo subjektai atlieka saugumo rizikos vertinimą, bet rizikos vertinimas dažnai atliekamas formaliai, siekiant atitikti teisės aktų reikalavimus ar tarptautiniu mastu pripažintų standartų nuostatas.

Prieš dvylika metų Lietuvos Respublikos vidaus reikalų ministerijos išleista metodinė priemonė „Rizikos analizės vadovas“ atspindi to laiko rizikos vertinimo mokslo ir inovacijų pažangą, tačiau saugumo rizikos vertinimo metodikos nuostatos ilgainiui kito ir iš kontrolės aplinkos užtikrinimo buvo pereita į visa apimantį organizacijos veiklos rizikos vertinimą.

9. Lietuvoje pavieniai įvairių saugumo sričių rizikos vertinimo procesai jau pasiekė brandą, tačiau nacionaliniu lygiu saugumo rizikos vertinimo kultūra, kibernetinio saugumo rizikos vertinimas tebėra fragmentiškas. Trūksta kibernetinių grėsmių ir saugumo spragų analizės visapusės integracijos į veiklos rizikos vertinimo procesus, o sparčiai plėtojantis IRT už kibernetinį saugumą atsakingam personalui pradeda trūkti rizikos vertinimo žinių, gebėjimų ir praktikos.

10. Siekiant tobulinti kibernetinio saugumo politikos formavimo ir įgyvendinimo kultūrą, atnaujinti kibernetinio saugumo rizikos vertinimo ir kitus reikalavimus, 2018 m. kibernetinio saugumo srityje įvyko šie reikšmingi pokyčiai:

10.1. Nauja redakcija išdėstytos Lietuvos Respublikos kibernetinio saugumo įstatymo nuostatos patobulino kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, patikslino kibernetinio saugumo politiką formuojančių ir įgyvendinančių institucijų kompetenciją, funkcijas, teises ir pareigas, kibernetinio saugumo subjektų pareigas bei atsakomybę ir nustatė papildomas kibernetinio saugumo užtikrinimo priemones.

10.2. Buvo sutelktos valstybės informacinių išteklių saugumo, viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veiklos reguliavimo ir saugumo funkcijos, o tai leidžia valstybėje užtikrinti sistemingą kibernetinės erdvės stebėjimą, jo valdymą ir atsakomybę; NKSC tapo vienintele Lietuvos institucija, organizuojančia kibernetinių incidentų valdymą šalyje ir vieno langelio principu teikiančia pagalbą valstybės institucijoms, verslui ir gyventojams.

11. Konsoliduojant pajėgumus, Lietuvoje siekiama kurti integralią kibernetinio saugumo vadybos sistemą, kuri įprasmintų sisteminį požiūrį į bet kurios srities saugumo vadybos planavimą, skatintų kibernetinio saugumo subjektų orientaciją į saugumo vadybos kokybės užtikrinimą, mažintų administracinę naštą kibernetinio saugumo subjektams, užtikrintų vertinimo sistemiškumą ir įrodymais pagrįstą saugumo valdymo kultūrą, padėtų optimizuoti saugumo išlaidų planavimą. Taip pat siekiama užtikrinti tolygią kibernetinio saugumo kompetencijų plėtrą ir regioninių kibernetinio saugumo pajėgumų stiprinimą.

12. Krašto apsaugos ministerija ir NKSC nuolat bendrauja su kibernetinio saugumo subjektais ir teikia konsultacijas kibernetinio saugumo tematika, rengia kibernetinio saugumo pratybas.

2017 m. nacionalinėse kibernetinio saugumo pratybose „Kibernetinis skydas 2017“ dalyvavo apie 200 atstovų iš daugiau nei 50 viešojo ir privataus sektorių organizacijų. Bendradarbiaujant su Lietuvos Respublikos ryšių reguliavimo tarnyba, Lietuvos policija ir Valstybine duomenų apsaugos inspekcija, pratybose dalyvaujančių kibernetinio saugumo subjektų atstovams surengti seminarai – supažindinta su kibernetinio saugumo srities teisės aktų reikalavimais. Pratybų dalyviai treniravosi suvaldyti ir atremti kibernetines atakas prieš ypatingos svarbos ryšių ir informacines sistemas ir užtikrinti šių sistemų funkcionavimą.

Krašto apsaugos ministerija ir toliau periodiškai rengs kompleksines nacionalines kibernetinio saugumo pratybas, skatins nuolatinį kibernetinio saugumo įgūdžių tobulinimą ne tik nacionalinėse, bet ir tarptautinėse kibernetinio saugumo pratybose.

13. Europos Sąjunga ir Šiaurės Atlanto sutarties organizacija (toliau – NATO) pripažįsta, kad kibernetinė erdvė pradedama naudoti kaip atskira karo erdvė arba kaip viena iš hibridinio karo priemonių. Kibernetinėmis priemonėmis jau galima sabotuoti valstybės ypatingos svarbos informacinės infrastruktūros veiklą (pvz., 2010 m. įvykdyta kibernetinė ataka Irano branduolinės energetikos objekte), neigiamai paveikti valstybės ir visuomenės saugumą (pvz., 2015 ir 2016 m. kibernetinės atakos Ukrainos elektros jėgainėse), ekonomiką ir socialinę gerovę, todėl nacionalinės kibernetinės erdvės saugumas yra kiekvienos valstybės nacionalinio saugumo interesas.

Pagal 2016 m. NATO viršūnių susitikimo Varšuvoje priimtą sprendimą dėl kibernetinės erdvės pripažinimo penktuoju kariavimo domenu Lietuvos kariuomenė tapo pagrindiniu Lietuvos Respublikos kibernetinės erdvės gynybos subjektu. Kibernetinės gynybos stiprinimas siekiant apsisaugoti nuo besivystančių karinių kibernetinių grėsmių ir efektyvus kibernetinių incidentų valdymas yra viena iš būtinų sąlygų užtikrinant gyvybinius ir pirmaeilius valstybės nacionalinio saugumo interesus. Įgyvendinant Lietuvos kariuomenei keliamus uždavinius, bus plėtojami nacionaliniai kibernetinės gynybos pajėgumai, užtikrinantys Lietuvos kariuomenės sąveiką su valstybės civiliniais pajėgumais, taip pat Lietuvos kariuomenės gebėjimai užtikrinti patikimą agresorių atgrasymą kibernetinėje erdvėje, o nepavykus atgrasyti – savarankiškai ir kartu su sąjungininkais ginti Lietuvos Respubliką karinėmis kibernetinio saugumo priemonėmis.

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, 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.

ANTRASIS SKIRSNIS
NUSIKALSTAMOS VEIKOS KIBERNETINĖJE ERDVĖJE

15. **Antrasis Strategijos tikslas** – užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą.

16. Nusikalstamos veikos kibernetinėje erdvėje daro didelį neigiamą poveikį pasaulio ekonomikai. Tyrimų duomenimis[2], pasaulinė nusikalstamų veikų kibernetinėje erdvėje padaryta žala siekia šimtus milijardų eurų per metus ir numatoma jos augimo tendencija. Nusikalstamas veikas darančius asmenis domina ne tik finansiniai, bet visi duomenys apskritai, todėl nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui, nurodytų Lietuvos Respublikos baudžiamojo kodekso XXX skyriuje, skaičius nuolat didėja (Nusikalstamų veikų žinybinio registro duomenimis, 2017 m. kibernetinėje erdvėje registruota 594 tokios nusikalstamos veikos, 2016 m. – 336). Europos policijos biure (toliau – Europolas) veikiančio

[2] Center for Strategic and International Studies, „McAfee“ (2018). *Economic Impact of Cybercrime – no slowing down,* Cybersecurity Ventures, Herjavec Group (2017). *2017 Cybercrime Report.*

Europos kovos su elektroniniu nusikalstamumu centro teigimu, su nusikalstamomis veikomis kibernetinėje erdvėje dažniausiai susiduria tos Europos Sąjungos valstybės, kuriose gerai išvystyta plačiajuosčio ryšio infrastruktūra ir veikia mokėjimo internetu sistemos[3].

17. „PwC“ kompanijos 2018 m. atlikto Pasaulio ekonominių nusikaltimų tyrimo (*Global Economic Crime Survey 2018*) duomenimis, 2018 m. sukčiavimo nusikaltimai kibernetinėje erdvėje buvo vieni iš dažniausių nusikaltimų, darančių didžiausią žalą privačiam sektoriui. Europole veikiantis Europos kovos su elektroniniu nusikalstamumu centras (EC3) prognozuoja, kad sparčiai vystantis IRT, socialinės inžinerijos metodams ir dėl kitų priežasčių nusikalstamų veikų kibernetinėje erdvėje skaičius vis didės. Be to, į kibernetinę erdvę persikelia vis daugiau nusikalstamų veikų, kurioms atlikti paprastai nebūtina naudoti IRT, pavyzdžiui, sukčiavimas, turto prievartavimas. Joms vykdyti ar pėdsakams slėpti pasitelkiami naujausi IRT sprendimai, kriptovaliutos, naudojamasi anoniminiame tinkle siūlomomis nusikalstamomis paslaugomis.

18. „Cybersecurity Ventures“ kompanija 2017 m. apskaičiavo, kad nusikalstamų veikų kibernetinėje erdvėje, kai naudojama kenkimo programinė įranga, daroma žala kasmet didėja, ir prognozuoja, kad pasaulis iki 2019 m. dėl išpirkos reikalaujančios kenkimo programinės įrangos plitimo patirs daugiau nei vienuolika milijardų dolerių vertės žalos. Europole veikiantis Europos kovos su elektroniniu nusikalstamumu centras (EC3) prognozuoja, kad ši žala ir toliau augs, ypač daugėjant daiktų interneto įrenginių *(Internet of Things (IoT)*. Nors kenkimo programinė įranga dažnai yra tik viena iš priemonių nusikalstamoms veikoms kibernetinėje erdvėje vykdyti, bet Europos tinklų ir saugumo agentūra (ENISA) 2018 m. paskelbtoje 2017 m. grėsmių paplitimo ataskaitoje *(ENISA Threat Landscape Report 2017)* šią kenkimo programinę įrangą jau kelerius metus iš eilės nurodo kaip dažniausią kibernetinę grėsmę.

19. Nusikalstamos veikos, susijusios su vaikų seksualiniu išnaudojimu kibernetinėje erdvėje, laikomos vienomis iš žalingiausių nusikalstamų veikų, kurioms plisti padeda sparčiai besivystančios IRT ir didėjančios naudojimosi jomis galimybės. Šios nusikalstamos veikos kibernetinėje erdvėje įgauna platesnį ir kompleksinį mastą ir jų skaičius, Nusikalstamų veikų žinybinio registro ir Europolo duomenimis Lietuvoje[4] ir Europoje[5], auga. Lietuva, siekdama užkardyti nusikalstamas veikas, susijusias su vaikų seksualiniu išnaudojimu kibernetinėje erdvėje, perkėlė 2011 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyvą 2011/92/ES dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija, kuria pakeičiamas Tarybos pamatinis sprendimas 2004/68/TVR (OL 2011 L 335, p. 1), ir 2012 m. spalio 2 d. ratifikavo Europos Tarybos 2007 m. spalio 25 d. konvenciją dėl vaikų apsaugos nuo seksualinio išnaudojimo ir seksualinės prievartos prieš juos (*Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*).

20. Siekiant užkardyti nusikalstamas veikas kibernetinėje erdvėje, peržengiančias valstybių sienas, svarbu plėtoti glaudų tarpvalstybinį bendradarbiavimą ir keitimąsi informacija,

---

[3] Europol's European Cybercrime Centre (EC3) (2017). *2017 Internet Organised Crime Threat Assessment (IOCTA)*

[4] Nusikalstamų veikų žinybinio registro duomenimis, 2016 m. buvo užregistruoti 123 nusikaltimai pagal Lietuvos Respublikos baudžiamojo kodekso 309 str. 2 d., 2017 m. – 132.

[5] European Union Agency for Law Enforcement Cooperation (Europol) (2017). *Europol Review 2016–2017.*

palaikyti ir gilinti santykius, pagrįstus tarptautiniais susitarimais ir naryste. Siekiant šio tikslo itin svarbi stipri politinė valia efektyviai vykdyti tarptautinius įsipareigojimus ir laikytis tarptautinių standartų užtikrinant kibernetinį saugumą ir kovojant su nusikalstamomis veikomis kibernetinėje erdvėje. Išreikšdama tokią politinę valią, Lietuva ratifikavo Europos Tarybos 2001 m. lapkričio 23 d. konvenciją dėl elektroninių nusikaltimų (*Convention on Cybercrime*) ir jos papildomus protokolus. Lietuva taip pat perkėlė 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyvą 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL 2013 L 218, p. 8). Įsipareigojimai sėkmingai vykdomi ne tik teisiniu, bet ir praktiniu lygiu, bendradarbiaujant su Tarptautine kriminalinės policijos organizacija (toliau – Interpolas) ir Interpolo pasauliniu inovacijų kompleksu, Europos Sąjungos agentūromis: Europos policijos biuru (Europolas), jo Europos kovos su elektroniniu nusikalstamumu centru (EC3) ir Europos teisminio bendradarbiavimo padaliniu (Eurojustas). Taip pat Lietuva dalyvauja nepertraukiamai veikiančių kontaktinių punktų kibernetinių nusikalstamų veikų tyrimo srityje tinklo, įsteigto remiantis Europos teisminiu tinklu (EJN) ir Budapešto konvencija, veikloje.

21. Nusikalstamoms veikoms kibernetinėje erdvėje nuolat evoliucionuojant, įgaunant naujų formų, teisėsaugos institucijų personalas, dirbantis šių nusikalstamų veikų tyrimo ir prevencijos srityje, turi būti tinkamai pasiruošęs įvertinti kibernetines grėsmes, identifikuoti nusikalstamas veikas kibernetinėje erdvėje ir efektyviai jas tirti. Labai svarbi ir tinkama prokuratūros, teismų darbuotojų ir šią veiklą organizuojančių ir jai vadovaujančių vadovų kompetencija. Tiriant šias veikas itin svarbūs teisėsaugos įstaigų gebėjimai surasti, užfiksuoti ir greitai ištirti elektroninius įrodymus.

22. **Uždaviniai antrajam Strategijos tikslui pasiekti**:

22.1. *Pirmasis antrojo tikslo uždavinys* – plėtoti valstybės pajėgumus ir gebėjimus kovoti su nusikalstamomis veikomis kibernetinėje erdvėje. Šis uždavinys bus įgyvendinamas tobulinant teisinę sistemą, stiprinant teisėsaugos institucijų profesinius gebėjimus tirti nusikalstamas veikas kibernetinėje erdvėje, kuriant analizės sistemas, diegiant pažangius veiklos metodus ir procedūras, techninius įrankius, skirtus kovai su nusikalstamomis veikomis kibernetinėje erdvėje.

22.2. *Antrasis antrojo tikslo uždavinys* – stiprinti nusikalstamų veikų kibernetinėje erdvėje prevenciją ir kontrolę. Šis uždavinys bus įgyvendinamas propaguojant visuomenės savisaugos kultūrą ir atsakingą elgesį kibernetinėje erdvėje, tobulinant teisėsaugos institucijų kovos su nusikalstamomis veikomis kibernetinėje erdvėje funkcijų vykdymą ir užtikrinant operatyvesnį tarptautinį bendradarbiavimą tiriant šias nusikalstamas veikas, plėtojant teisėsaugos institucijų efektyvų bendradarbiavimą su mokslo ir studijų institucijomis, viešojo ir privataus sektorių atstovais bei visuomene.

TREČIASIS SKIRSNIS
KIBERNETINIO SAUGUMO KULTŪRA IR INOVACIJOS

23. **Trečiasis Strategijos tikslas** – skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą.

24. Kibernetiniai incidentai šiuolaikiniame pasaulyje yra neišvengiami, nuo jų negalima apsisaugoti net ir taikant visas esamas technines kibernetinio saugumo priemones, todėl viešojo ir privataus sektorių atstovai turi rūpintis savo darbuotojų kibernetinės kultūros kėlimu. IBM įmonės 2017 m. atlikto tyrimo[6] duomenimis, daugėja kibernetinių incidentų, kurie buvo sukelti per tiriamo privataus sektoriaus darbuotojų aplaidumą ar nežinojimą (2017 m. tokie kibernetiniai incidentai sudarė daugiau nei 20 proc., 2016 m. – 15 proc.). Daugiau nei trečdalis tokių kibernetinių incidentų įvyko, nes darbuotojai atvėrė teisės pažeidėjų atsiųstas nuorodas ar su elektroniniu laišku atsiųstus dokumentus. Lietuvoje taip pat daugėja elektroninių laiškų, sukurtų taikant socialinės inžinerijos metodus[7].

25. 2018 m. Europos inovacijų diegimo rezultatų suvestinės duomenimis, Europoje privataus sektoriaus atstovai vis daugiau dėmesio skiria darbuotojų IRT srities mokymams, tačiau Lietuvoje šis rodiklis tik truputį viršija 10 proc. (rodiklio vidurkis Europoje – 21 proc.). Valstybės tarnautojams Lietuvoje taip pat sudaryta galimybė tobulinti įgūdžius kibernetinio saugumo srityje. Kibernetinio saugumo kursus išklausiusių valstybės tarnautojų skaičius kiekvienais metais didėja (Valstybės tarnybos departamento duomenimis, 2015 m. kursus išklausė 146 valstybės tarnautojai, 2016 m. – 249, 2017 m. – 289), bet reguliarūs viešojo ir privataus sektorių darbuotojų kibernetinio saugumo mokymai, organizuojami atsižvelgiant į naujausias kibernetinio saugumo tendencijas Lietuvoje ir pasaulyje, padidintų darbuotojų atidumą ir kibernetinio saugumo kultūrą.

26. Siekiant kelti Lietuvos gyventojų kibernetinio saugumo kultūrą, turi būti užtikrinta nuolatinė informacijos sklaida, apimanti aktualią informaciją apie naujausius kibernetinius incidentus ir kitus veiksnius, galinčius sukelti grėsmę asmens duomenų saugumui ar tapti nusikalstamų veikų kibernetinėje erdvėje aukomis. 2017 m. specialaus Eurobarometro 464a tyrimo, skirto europiečių požiūriui į kibernetinį saugumą nustatyti, duomenimis, tik 16 proc. interneto vartotojų Lietuvoje mano, kad rizika tapti nusikalstamų veikų kibernetinėje erdvėje aukomis nedidėja (Europos Sąjungos vidurkis – 11 proc.), tačiau šios srities informacijos sklaida turėtų būti didesnė, nes 49 proc. interneto vartotojų Lietuvoje jaučiasi per mažai informuoti apie nusikalstamų veikų kibernetinėje erdvėje riziką (Europos Sąjungos vidurkis – 51 proc.).

27. Pasaulyje atlikta daug tyrimų ir prognozių, jų išvadose konstatuojama esama ir būsima kibernetinio saugumo įgūdžių stoka[8]. Reikiamą kompetenciją gali užtikrinti kokybiškas ir darbo rinkos poreikius atitinkantis švietimas. Šiuo metu Lietuvoje kibernetinio saugumo

---

[6] IBM. *IBM X-Force Threat Intelligence Index 2018 (2018).*
[7] Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (2018). *2017 m. Nacionalinio kibernetinio saugumo būklės ataskaita*.
[8] ISACA. *State of Cybersecurity 2018 (2018),* Information Security Community on LinkedIn, $(ISC)^2$. *Cybersecurity Trends. 2017 Spotlight Report (2017).*

programas siūlo keturi universitetai, tačiau, remiantis asociacijos „Infobalt“ ir VšĮ „Investuok Lietuvoje“ 2018 m. atlikto tyrimo „IRT specialistai Lietuvoje: situacija darbo rinkoje ir darbdavių poreikiai“ duomenimis, padėtis neatitinka darbo rinkos poreikių, todėl, siekiant sumažinti didėjantį atotrūkį tarp kibernetinio saugumo specialistų paklausos ir pasiūlos, turi būti plėtojamos ir stiprinamos esamos ir kuriamos naujos studijų programos, skirtos kibernetinio saugumo specialistams rengti.

Siekiant aukštesnės kibernetinio saugumo kultūros, svarbu, kad su kibernetinio saugumo pagrindais būtų supažindinami ikimokyklinio ugdymo įstaigų ugdytiniai ir bendrojo lavinimo mokyklų mokiniai, nes IRT vis plačiau naudojamos užtikrinant ugdymo ir mokymosi procesą.

Įgyvendinant Lietuvos Respublikos Vyriausybės programoje numatytą pedagogų rengimo bei kvalifikacijos tobulinimo sistemos pertvarkymą, taip pat turėtų būti siekiama kelti pedagogų kvalifikaciją kibernetinio saugumo srityje, nes tik kompetentingi įvairių ugdymo sričių pedagogai gebės gerai parengti studentus praktiniam darbui ir taip prisidės prie žiniomis ir inovacijomis grįstos visuomenės kūrimo, taip pat ir kibernetinio saugumo didinimo.

28. Daugelio kibernetinio saugumo ekspertų nuomone[9], pasaulyje iki 2019 m. bus mažiausiai 1,5 milijono laisvų kibernetinio saugumo specialistų darbo vietų. Asociacijos „Infobalt“ ir VšĮ „Investuok Lietuvoje“ 2018 m. atlikto tyrimo „IRT specialistai Lietuvoje: situacija darbo rinkoje ir darbdavių poreikiai“ duomenimis, IRT specialistų skaičius Lietuvoje siekia 22,6 tūkst., per ateinančius trejus metus privačiame sektoriuje papildomai reikės apie 13,3 tūkst. įvairių IRT specialistų. Tyrėjai nepateikė duomenų apie kibernetinio saugumo specialistų trūkumą Lietuvoje, tačiau galima daryti prielaidą, kad kibernetinio saugumo specialistai sudaro reikšmingą trūkstamų specialistų dalį. Sprendžiant kibernetinio saugumo specialistų trūkumo problemą, pirmiausia reikėtų nustatyti, kokių kibernetinio saugumo specialistų šalyje trūksta labiausiai, nes, remiantis kitose valstybėse atliktų tyrimų išvadomis[10], skirtingose valstybėse kibernetinio saugumo specialistų poreikis gali būti skirtingas, gali skirtis ir problemos, susijusios su kibernetinio saugumo įgūdžių stoka, be to, specialistų stokojama ne visose kibernetinio saugumo srityse.

29. Sparčiai plečiantis kibernetinei erdvei atsiranda galimybių diegti inovacijas, kurios yra produktyvumo ir ekonomikos augimo variklis: sudaro galimybes kurti naujų ir geresnių darbo vietų, didina socialinį mobilumą ir yra atsakas į globalius socialinius ir saugumo iššūkius.

Lietuva palyginti neseniai įstojo į Europos Sąjungą, todėl čia nėra gilių kibernetinio saugumo mokslinių tyrimų ir mokymo tradicijų, – jos sutelktos kitose Europos Sąjungos valstybėse. Lietuva turi daug galimybių geriau pasinaudoti Europos Sąjungos teikiama investicijų į mokslinius tyrimus skatinimo galimybe – bendrąja mokslinių tyrimų ir inovacijų programa „Horizontas 2020“ (2014–2020 m.) – ir taip prisidėti prie skaitmeninės ekonomikos kūrimo ir gynybos politikos stiprinimo nacionaliniu ir Europos Sąjungos lygiu. Valstybės pastangos turi būti orientuotos į įvairias paramos priemones, suteikiančias įmonėms daugiau

[9] Silensec. *Addressing the Cyber Security Skills Gap (2017).*
[10] Indeed. *Indeed Spotlight: The Global Cybersecurity Skills Gap (2017),* Information Security Community on LinkedIn, (ISC)^2. *Cybersecurity Trends. 2017 Spotlight Report (2017)*

galimybių įsitraukti į tarptautinius tinklus, ieškant potencialių darbuotojų ir partnerių. Tai paskatintų privatų sektorių investuoti į mokslinių tyrimų, eksperimentinės plėtros ir inovacijų sritis, kurti naujus produktus ir paslaugas, taip pat ir kibernetinio saugumo srityje. Inovatyvių kibernetinio saugumo produktų kūrimas suteiktų papildomą postūmį, paskatintų Lietuvos pramonės konkurencingumą ir yra būtinas siekiant atremti šiuolaikinius kibernetinius incidentus. Taip pat svarbu skatinti Lietuvos mokslininkų dalyvavimą rengiant tarptautines bendras mokslines publikacijas kibernetinio saugumo srityje, pritraukti daugiau studentų, tiesiogiai dalyvauti aukšto lygio kibernetinio saugumo srityje moksliniuose tyrimuose ir eksperimentinės plėtros projektuose, plėtoti viešojo, privataus sektorių ir mokslo institucijų bendradarbiavimą, padidinti užsienio doktorantų kibernetinio saugumo srityje skaičių.

30. 2018 m. Europos inovacijų diegimo rezultatų suvestinės duomenimis, Lietuva, palyginti su kitomis Europos Sąjungos valstybėmis narėmis, yra nuosaikioji inovatorė, tačiau padariusi didelę pažangą skatindama inovacijas ir gerindama inovacijų ekosistemą[11]. Europos Sąjungoje privatus sektorius inovacijoms vis dar skiria mažiau lėšų nei jų konkurentai už Europos Sąjungos ribų. Lietuvoje dar neatlikti patikimi kibernetinio saugumo rinkos matavimai, bet pripažįstama, kad ši rinka yra auganti, todėl inovacijos čia padėtų nuosekliai kurti ir stiprinti konkurencingos šalies, kuriančios inovatyvius kibernetinio saugumo produktus ir paslaugas, statusą. Šios sinergijos galima siekti jungiant inovacijų iniciatyvas su bendrąja valstybės politika, siekiant ilgalaikės mokslo, technologijų ir inovacijų plėtros.

31. Lietuvoje sudaryta finansinių paslaugų veiklai palanki reguliacinė ir priežiūros aplinka, skatinanti inovacijas finansų sektoriuje. Remiantis ataskaitos „Lithuania Fintech Report 2017“ duomenimis, 2017 m. Lietuvoje veikė 117 finansinių technologijų (*FinTech*) įmonių. Ši sritis yra viena iš strateginių Lietuvos banko veiklos krypčių, tad jo veikla vienoje perspektyviausių finansinių technologijų inovacijų – blokų grandinės technologijų (*Blockchain*) – srityje veiksmingai prisidės plėtojant finansinių technologijų inovacijas.

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 srities mokymų, akreditavimo ir sertifikavimo sistemas, orientuotas į darbo rinkos poreikius, pritraukiant ir ugdant talentus, kuriant kibernetinio saugumo mokymų ir testavimo aplinką,

[11] Europos Komisija. 2018 m. Europos inovacijų diegimo rezultatų suvestinė (2018).

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.

KETVIRTASIS SKIRSNIS
PRIVATAUS IR VIEŠOJO SEKTORIŲ BENDRADARBIAVIMAS

33. **Ketvirtasis Strategijos tikslas** – stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą.

34. Šiuolaikinėse valstybėse, kuriose gerai išvystyta plačiajuosčio ryšio infrastruktūra, viešojo sektoriaus atstovai nebegali toliau vieni kovoti su pavojingais ar didelės reikšmės kibernetiniais incidentais, o ypatingos svarbos informacinės infrastruktūros valdytojai – neretai privataus sektoriaus atstovai – patys ne visada gali suvaldyti kibernetinius incidentus, dažnai peržengiančius jų organizacijos ribas. Taigi privataus ir viešojo sektorių bendradarbiavimas tampa būtina sąlyga visapusiškam kibernetiniam saugumui užtikrinti. Privataus ir viešojo sektorių efektyvaus bendradarbiavimo esminė sąlyga – visavertė partnerystė: abipusis pasitikėjimas ir nauda, todėl privataus ir viešojo sektorių bendradarbiavimas turėtų būti į tai orientuotas.

35. Lietuvos Respublikos Vyriausybės 2015 m. balandžio 23 d. nutarimu Nr. 422 „Dėl Kibernetinio saugumo tarybos sudarymo ir jos reglamento patvirtinimo“ sudaryta Kibernetinio saugumo taryba yra privataus ir viešojo sektorių bendradarbiavimo politiniu lygmeniu pavyzdys. Turi būti siekiama tobulinti Kibernetinio saugumo tarybos veiklą plečiant privataus ir viešojo sektorių bendradarbiavimą, efektyviai naudojantis Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytomis Kibernetinio saugumo tarybos teisėmis.

36. Privataus ir viešojo bendradarbiavimo įgyvendinimui užtikrinti naudojamas Kibernetinio saugumo informacinis tinklas (toliau – tinklas). Vienas iš tinko tikslų yra dalytis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir tinklo narių bendradarbiavimą kibernetinio saugumo srityje. Tinkle būtina įdiegti priemones, užtikrinančias efektyvų ir abipusį pasitikėjimą skatinantį tinklo narių bendravimą.

37. IRT taikomos labai plačiai ir jų nauda XXI amžiuje neabejotina, tačiau IRT paplitimas kelia klausimą, kaip efektyviai reaguoti į aptiktas IRT saugumo spragas. IRT saugumo spragų ieško asmenys, turintys skirtingų tikslų, tačiau, siekiant atsakingumo atskleidžiant IRT saugumo spragas, svarbu sudaryti galimybę saugumo spragą suradusiam ir

norinčiam ją ištaisyti asmeniui bendradarbiauti su kibernetinio saugumo subjektais, kurių IRT saugumo spraga buvo atskleista. Kibernetinio saugumo subjektai, nustatę ir viešai paskelbę IRT saugumo spragų atskleidimo tvarką, apsisaugotų nuo kibernetinių incidentų galimos žalos arba ją labai sumažintų. IRT saugumo spragų atskleidimo tvarkos nustatymas ir viešas paskelbimas prisidėtų prie valstybės kibernetinio saugumo užtikrinimo ir sudarytų daugiau privataus ir viešojo sektorių bendradarbiavimo galimybių.

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 IRT spragų atskleidimo praktiką, nustatant šios srities veiklos principus, metodų, techninių gebėjimų ar kitų priemonių taikymo tvarką.

PENKTASIS SKIRSNIS
TARPTAUTINIS BENDRADARBIAVIMAS

39. **Penktasis Strategijos tikslas** – stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą.

40. Lietuvos nacionalinis saugumas ir visuomenės gerovė tiesiogiai priklauso nuo stabilios, laisvai prieinamos ir saugios kibernetinės erdvės. Atsižvelgdama į tarpvalstybinį, sienų nepaisantį kibernetinių grėsmių ir rizikos pobūdį, Lietuva sieks stiprinti nacionalinį kibernetinį saugumą, aktyviai bendradarbiaudama su dvišaliais ir daugiašaliais partneriais ir tikslingai veikdama tarptautiniuose forumuose, skirtuose kibernetinio saugumo bei pasaulinės interneto erdvės valdymo problemoms spręsti.

41. Lietuva siekia tapti aktyvia kibernetinio saugumo ir interneto valdymo klausimus sprendžiančios tarptautinės bendruomenės dalimi, aktyviai bendradarbiauti su partneriais ir sąjungininkais, sudarant tarptautinį sutarimą dėl teisinio kibernetinės erdvės reguliavimo, pagrįsto tarptautinės teisės normų laikymusi, veiklos šioje erdvėje principų ir normų, atviro

interneto apsaugos, žmogaus teisių bei laisvių apsaugos skaitmeninėje erdvėje. Ypač daug dėmesio Lietuva skirs bendradarbiavimui kibernetinės gynybos srityje su NATO, Europos Sąjungos ir kitomis demokratinių principų besilaikančiomis šalimis. Lietuva pasisako už kuo artimesnį ir darnų NATO ir Europos Sąjungos bendradarbiavimą šioje srityje, siekiant išvengti funkcijų ir veiklų dubliavimosi. Lietuva stiprins dvišalį politinio ir techninio lygmens bendradarbiavimą, ypač su Jungtinėmis Amerikos Valstijomis.

42. **Uždaviniai penktajam Strategijos tikslui pasiekti:**

42.1. *Pirmasis penktojo tikslo uždavinys* – plėtoti tarptautinį, tarpvalstybinį ir Baltijos regiono šalių bendradarbiavimą kibernetinio saugumo srityje. Šis uždavinys bus įgyvendinamas dalyvaujant Europos Sąjungos, NATO, Jungtinių Tautų, Europos saugumo ir bendradarbiavimo organizacijos, Baltijos regiono ir kitų tarptautinių organizacijų veikloje.

42.2. *Antrasis penktojo tikslo uždavinys* – stiprinti tarptautinius kibernetinio saugumo pajėgumus ir gebėjimus. Šis uždavinys bus įgyvendinamas inicijuojant Nuolatinio struktūrizuoto bendradarbiavimo projektą ir jam vadovaujant, siekiant stiprinti Europos Sąjungos valstybių narių, kurių civiliniai ir kariniai pajėgumai atitinka aukštesnius kriterijus ir kurios tarpusavyje yra susaistytos didesniais įsipareigojimais, bendradarbiavimą kibernetinio saugumo ir gynybos srityje.

42.3. *Trečiasis penktojo tikslo uždavinys* – plėsti dialogą su Jungtinėmis Amerikos Valstijomis kibernetinės gynybos srityje, siekti Jungtinių Amerikos Valstijų dalyvavimo Lietuvos kibernetinio saugumo užtikrinimo projektuose. Šis uždavinys bus įgyvendinamas plėtojant dvišalį Lietuvos ir Jungtinių Amerikos Valstijų politinio ir techninio lygmens bendradarbiavimą kibernetinės gynybos ir saugumo srityje, kartu su Jungtinėmis Amerikos Valstijomis vykdant veiklas, stiprinančias mūsų šalies kibernetinę gynybą ir saugumą.

IV SKYRIUS
STRATEGIJOS ĮGYVENDINIMAS IR ATSAKOMYBĖ

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.

45. Strategija įgyvendinama iš atitinkamų metų Lietuvos Respublikos valstybės biudžeto asignavimų, savivaldybių biudžetų lėšų, Europos Sąjungos ir kitos tarptautinės finansinės paramos lėšų ir kitų teisėtai gautų lėšų. Už reikalingų finansinių išteklių planavimą,

vadovaujantis Lietuvos Respublikos kibernetinio saugumo įstatyme įtvirtintu subsidarumo principu, pagal kompetenciją atsako Strategijos vykdytojai.

46. Strategijos tikslų pasiekimas vertinamas pagal Strategijos įgyvendinimo vertinimo kriterijus ir siekiamas jų reikšmes, nurodytus Strategijos priede. Atliekant Strategijos įgyvendinimo stebėseną ir vertinimą taip pat bus naudojami viešai skelbiami Lietuvos statistikos departamento, Eurostato, sociologinių apklausų ir tyrimų duomenys. Strategijos įgyvendinimo rezultatų stebėseną atlieka Krašto apsaugos ministerija, NKSC ir Kibernetinio saugumo taryba.

47. Strategijos vykdytojai, pasibaigus metams, ne vėliau kaip iki kitų metų sausio 15 d. NKSC pateikia informaciją apie Strategijos įgyvendinimo eigą, veiksmingumą ir tai pagrindžiančius duomenis. Kartu su šia informacija gali būti pateikti siūlymai dėl Strategijos ir (arba) jos įgyvendinamųjų dokumentų tikslinimo. NKSC prašymu Strategijos vykdytojai privalo pateikti ir kitą Strategijos įgyvendinimo rezultatų stebėsenai būtiną informaciją. Visi suinteresuoti subjektai gali teikti pasiūlymus dėl Strategijos nuostatų atnaujinimo visą jos įgyvendinimo laikotarpį.

48. Gavęs Strategijos 49 punkte nurodytą informaciją, NKSC ne vėliau kaip iki einamųjų metų vasario 1 d. Krašto apsaugos ministerijai pateikia susistemintus duomenis apie praėjusių metų Strategijos tikslų ir uždavinių įgyvendinimo būklę, gautus pasiūlymus ir problemines sritis, trukdančias įgyvendinti Strategiją.

49. Krašto apsaugos ministerija kasmet iki kovo 1 d. apibendrina gautą praėjusių metų informaciją ir duomenis apie Strategijos įgyvendinimo eigą, veiksmingumą, susistemintus duomenis apie Strategijos metinį įgyvendinimą pristato Kibernetinio saugumo tarybai ir pateikia Lietuvos Respublikos Vyriausybei. Vyriausybė dėl Strategijos įgyvendinimo kiekvienais metais atsiskaito Lietuvos Respublikos Seimui pateikdama Nacionalinio saugumo būklės ir plėtros metinę ataskaitą.

50. Visa vieša informacija, susijusi su metiniu ir galutiniu Strategijos įgyvendinimo vertinimu, skelbiama NKSC interneto svetainėje.

51. Likus pusei metų iki nustatyto Strategijos įgyvendinimo laikotarpio pabaigos, NKSC parengia ir Krašto apsaugos ministerijai pateikia Strategijos galutinį įgyvendinimo vertinimą, kuris pristatomas Kibernetinio saugumo tarybai ir pateikiamas Lietuvos Respublikos Vyriausybei.

_____

Nacionalinės kibernetinio saugumo
strategijos
priedas

NACIONALINĖS KIBERNETINIO SAUGUMO STRATEGIJOS ĮGYVENDINIMO VERTINIMO KRITERIJAI IR SIEKIAMŲ JŲ REIKŠMIŲ SĄRAŠAS

Eil. Nr.	Vertinimo kriterijaus pavadinimas	Vertinimo kriterijaus reikšmė			Vertinimo kriterijaus pasiekimo stebėseną atliekanti institucija ar įstaiga
		Pradinė žinoma reikšmė 2017 m.	2021 m.	2023 m.	
Nacionalinės kibernetinio saugumo strategijos (toliau – Strategija) **pagrindinis tikslas** yra efektyviai ir laiku identifikuojant kibernetinius incidentus, užkertant kelią jų atsiradimui ir plitimui, valdant kibernetinių incidentų sukeltas pasekmes užtikrinti galimybę Lietuvos visuomenei saugiai naudotis IRT teikiamomis galimybėmis					
1.	Lietuvos Respublikos vieta pasauliniame kibernetinio saugumo indekse, ne mažesnė nei nurodyta	57	30	20	Krašto apsaugos ministerija
2.	Kibernetinių incidentų grėsmės lygis, ne didesnis nei nurodyta	3,4	3,2	3	Krašto apsaugos ministerija
Pirmasis Strategijos tikslas – stiprinti valstybės kibernetinį atsparumą ir kibernetinių gynybos pajėgumų plėtrą					
3.	Kibernetinio saugumo reikalavimus atitinkančių kibernetinių saugumo subjektų dalis procentais, ne mažesnė nei nurodyta	*	35	50	Krašto apsaugos ministerija
4.	Viešojo sektoriaus interneto svetainių, į kurias sunku įsilaužti, dalis procentais, ne mažesnė nei nurodyta	25	28	32	Krašto apsaugos ministerija
5.	Nacionalinėse kibernetinio saugumo pratybose dalyvaujančių ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių valdytojų dalis, ne mažesnė nei nurodyta	42	60	70	Krašto apsaugos ministerija
6.	Modernizuoti valstybės kibernetinės gynybos pajėgumai procentais, ne mažiau nei nurodyta	RN	RN	RN	Krašto apsaugos ministerija
Antrasis Strategijos tikslas – užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą					
7.	Mokymus baigusių pareigūnų, prokurorų, specialistų, ekspertų, dalyvaujančių tiriant nusikalstamas veikas kibernetinėje erdvėje, dalis procentais, ne mažesnė nei nurodyta	*	70	90	Krašto apsaugos ministerija kartu su Strategijos vykdytojais

Eil. Nr.	Vertinimo kriterijaus pavadinimas	Vertinimo kriterijaus reikšmė			Vertinimo kriterijaus pasiekimo stebėseną atliekanti institucija ar įstaiga
		Pradinė žinoma reikšmė 2017 m.	2021 m.	2023 m.	
8.	Sukurtų ar įdiegtų techninių įrankių, procedūrų, analizės platformų, skirtų kovai su nusikalstamomis veikomis kibernetinėje erdvėje, skaičius vienetais, ne mažesnis nei nurodyta	*	2	5	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
9.	Projektų, skirtų nusikalstamų veikų kibernetinėje erdvėje prevencijai ir kontrolei stiprinti, skaičius vienetais, ne mažesnis nei nurodyta	2	2	2	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
10.	Dalyvavimo nusikalstamų veikų kibernetinėje erdvėje prevencijos ir tyrimo tarptautiniuose renginiuose ir darbo grupėse skaičius vienetais, ne mažesnis nei nurodyta	12	14	15	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
11.	Dalyvavimo tarptautinėse operacijose, tiriant nusikalstamas veikas kibernetinėje erdvėje, skaičius vienetais, ne mažesnis nei nurodyta	3	4	6	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
Trečiasis Strategijos tikslas – skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą					
12.	Kibernetinio saugumo srities inovacijų plėtrą skatinančių projektų skaičius, iš viso nuo 2018 m.	0	5	10	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
13.	Investicijų į kibernetinio raštingumo kultūros skatinimą, saugumo žinių, mokslinių tyrimų plėtrą, suma tūkstančiais eurų, ne mažesnė nei nurodyta	*	1 000	2 000	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
14.	Asmenų, įgijusių kibernetinio saugumo kvalifikaciją, skaičius vienetais, ne mažesnis nei nurodyta.	33	200	400	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
15.	Per Valstybės tarnautojų registro ir valstybės tarnybos valdymo informacinės sistemos modulį mokytų institucijų ir įstaigų valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis, dalis procentais, ne mažesnė nei nurodyta	0	10	70	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
Ketvirtasis Strategijos tikslas – stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą					
16.	Sukurtas viešojo ir privataus sektorių bendradarbiavimo kibernetinio saugumo srityje modelis, vienetais	-	-	1	Krašto apsaugos ministerija kartu su

Eil. Nr.	Vertinimo kriterijaus pavadinimas	Vertinimo kriterijaus reikšmė			Vertinimo kriterijaus pasiekimo stebėseną atliekanti institucija ar įstaiga
		Pradinė žinoma reikšmė 2017 m.	2021 m.	2023 m.	
					Strategijos vykdytojais
17.	Įtrauktų į kibernetinio saugumo informacinį tinklą valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros valdytojų dalis procentais, ne mažesnė nei nurodyta	36	86	90	Krašto apsaugos ministerija
18.	Priemonių, skirtų mažų ir vidutinių viešojo ir privataus sektorių organizacijų kibernetinio saugumo būklei gerinti, skaičius vienetais, ne mažesnis nei nurodyta	0	4	6	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
19.	Priemonių, skirtų atsakingai viešojo ir privataus sektorių pažeidžiamumo atskleidimo praktikai formuoti, skaičius vienetais, ne mažesnis nei nurodyta	0	1	2	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
Penktasis Strategijos tikslas – stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą					
20.	Dalyvavimo Europos Sąjungos, NATO, Baltijos regiono organizuojamuose susitikimuose, forumuose ar kituose renginiuose kibernetinio saugumo tema, į kuriuos buvo kviečiama, dalis procentais, ne mažesnė nei nurodyta	25	50	70	Krašto apsaugos ministerija kartu su Strategijos vykdytojais
21.	Dalyvavimo tarptautinėse kibernetinių incidentų tyrimo organizacijų darbo grupių susitikimuose, į kuriuos buvo kviečiama, dalis procentais, ne mažesnė nei nurodyta	70	85	100	Krašto apsaugos ministerija
22.	Pasirašytų bendradarbiavimo susitarimų su tarptautinėmis organizacijomis, Europos Sąjungos, NATO, Baltijos regiono ir kitomis šalimis kibernetinio saugumo srityje skaičius vienetais, ne mažesnis nei nurodyta	*	1	2	Krašto apsaugos ministerija kartu su Strategijos vykdytojais

*Pradinė atitinkamo Strategijos įgyvendinimo vertinimo kriterijaus reikšmė nežinoma, nes institucijos, koordinuojančios tam tikro vertinimo kriterijaus atitiktį, neturi duomenų apie šių vertinimo kriterijų reikšmes. Duomenys apie vertinimo kriterijaus reikšmę bus renkami 2019 m.

_____