Projektas

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS
DĖL NACIONALINĖS KIBERNETINIO SAUGUMO STRATEGIJOS PATVIRTINIMO

Nr.
Vilnius

Vadovaudamasi Lietuvos Respublikos kibernetinio saugumo įstatymo 5 straipsnio 1 punktu ir įgyvendindama Europos Parlamento ir Tarybos direktyvos 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194, 1–30) 7 straipsnio 1 dalį, Lietuvos Respublikos Vyriausybė n u t a r i a:

1. Patvirtinti Nacionalinę kibernetinio saugumo strategiją (pridedama).
2. Pripažinti netekusiu galios Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimą Nr. 796 „Dėl Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“.

Ministras Pirmininkas

Krašto apsaugos ministras

Užsienio reikalų ministras
Linas Linkevičius

KAM Administracijos departamento
Dokumentų administravimo skyriaus
vyr. specialistė
Vesta Adomaitienė

Teisės departamento
Įstaigų teisinės priežiūros skyriaus
vedėjas
Antanas Aleknavičius

Krašto apsaugos viceministras
Edvinas Kerza

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
nutarimu Nr.

NACIONALINĖ KIBERNETINIO SAUGUMO STRATEGIJA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinė kibernetinio saugumo strategija (toliau – Strategija) parengta siekiant nustatyti nacionalinio kibernetinio saugumo užtikrinimo tikslus ir uždavinius, užtikrinti veiksmingą ir kryptingą kibernetinio saugumo sistemos plėtrą Lietuvos Respublikoje iki 2023 m.

2. Strategija nustato svarbiausias nacionalinės kibernetinio saugumo politikos viešajame ir privačiame sektoriuose nuostatas ir orientuojama į valstybės kibernetinio atsparumo didinimą, kibernetinių gynybos pajėgumų plėtrą, kibernetinio saugumo kultūros plėtojimą, viešojo ir privataus sektoriaus bendradarbiavimo stiprinimą, kovos su nusikaltimais kibernetinėje erdvėje efektyvinimą ir tarptautinio bendradarbiavimo plėtojimą.

3. Valstybės kibernetinis atsparumas suprantamas kaip viešojo ir privataus sektoriaus organizacijų, gyventojų gebėjimas nustatyti kibernetines grėsmes, užkirsti kelią jų plitimui, valdyti grėsmių sukeltas pasekmes ir neleisti joms kartotis.

4. Strategija parengta atsižvelgiant į aplinkos analizę, tyrimų rezultatus, visuomenės, valstybės ir savivaldybių įstaigų 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 Nr. XII-1428, Europos Parlamento ir Tarybos direktyvos 2016/1148 „Dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti“, 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.

5. Strategijoje vartojamos sąvokos atitinka Lietuvos Respublikos kibernetinio saugumo įstatyme apibrėžtas sąvokas.

II SKYRIUS
KIBERNETINIO SAUGUMO STRATEGIJOS PRINCIPAI

6. Įgyvendinant Strategijos nuostatas, visuomenės, verslo subjektų ir valstybės institucijų veikla turi būti grindžiama šiais principais:

6.1. **kibernetinės erdvės nediskriminavimo** – teisės aktų nuostatos yra taikomos, o gėriai saugomi vienodai ir fizinėje, ir kibernetinėje erdvėje;

6.2. **kibernetinio saugumo kaip nacionalinio saugumo sistemos visumos** – tai vienas iš valstybės raidos tvarumo elementų, kurių visuma priskiriama prie pirmaeilių valstybės nacionalinio saugumo interesų, kurių neginant ilgainiui būtų pažeisti gyvybiniai Lietuvos Respublikos interesai;

6.3. **kibernetinio saugumo rizikos valdymo** – taikomos kibernetinio saugumo priemonės turi užtikrinti kibernetinio saugumo subjektų reguliariai įvertinamos rizikos suvaldymą;

6.4. **kibernetinio saugumo proporcingumo** – taikomi teisiniai, organizaciniai ir techniniai kibernetinio saugumo reikalavimai neturi apriboti kibernetinio saugumo subjektų veiklos kibernetinėje erdvėje labiau, negu tai būtina;

6.5. **viešojo intereso viršenybės** – taikomos kibernetinio saugumo užtikrinimo priemonės pirmiausia turi užtikrinti visuomenės viešojo intereso apsaugą, bet neturi iš esmės pažeisti atskirų vartotojų teisių ar neproporcingai apriboti jų laisvės kibernetinėje erdvėje;

6.6. **inovacijų skatinimo** – kuriant pažangiausius kibernetinio saugumo produktus turi būti atsižvelgiama į naujausias ir aktualiausias kibernetines grėsmes, o kūrimo procesas turi aprėpti visus etapus nuo idėjos koncepcijos patikrinimo iki produkto parengimo rinkai;

6.7. **standartizacijos ir technologinio neutralumo** – įgyvendinant kibernetinio saugumo užtikrinimo priemones, kibernetinio saugumo subjektai skatinami vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais ryšių ir informacinių sistemų kibernetinio saugumo standartais ir specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės;

6.8. **subsidiarumo** – už ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakingi šias sistemas valdantys ir paslaugas teikiantys kibernetinio saugumo subjektai. Srityse, kurios priklauso išimtinai kibernetinio saugumo subjektų kompetencijai, kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos veiksmų imasi tik tada, kai ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinio saugumo negali užtikrinti šias sistemas valdantys ir paslaugas teikiantys kibernetinio saugumo subjektai.

7. Šiame skyriuje nurodyti principai įgyvendinant Strategiją turi būti derinami tarpusavyje, nė vienam iš jų iš anksto nesuteikiama pirmenybė.

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

8. Strategijos pagrindinis tikslas – bendradarbiaujant visuomenei, viešajam ir privačiam sektoriui, mokslo ir švietimo institucijoms tarpusavyje ir su tarptautinių organizacijų kompetentingomis institucijomis, jų įsteigtomis bendradarbiavimo grupėmis bei užsienio valstybių kompetentingomis institucijomis ir tarnybomis, dalijantis atsakomybe kibernetinio saugumo srityje, reikšmingai sustiprinti valstybės kibernetinį atsparumą ir valstybės kibernetinę gynybą bei numatyti tam reikalingus išteklius siekiant ekonominės ir socialinės gerovės.

PIRMASIS SKIRSNIS
VALSTYBĖS KIBERNETINIS ATSPARUMAS IR KIBERNETINIAI GYNYBOS PAJĖGUMAI

9. **Pirmasis Strategijos tikslas** – stiprinti valstybės kibernetinį atsparumą ir kibernetinių gynybos pajėgumų plėtrą.

10. Valstybė, taikydama rizikos vertinimu pagrįstą požiūrį, pagal galimybes ir įgaliojimus siekia stiprinti kibernetinį atsparumą ir užtikrinti savo kibernetinių gynybos pajėgumų plėtrą, kurdama sisteminį požiūrį į kibernetinį saugumą, vykdydama prevencinę veiklą, didindama kibernetinio saugumo politikos formavimo ir įgyvendinimo efektyvumą, skatindama kibernetinio saugumo pratybų vykdymą, stiprindama viešojo ir privataus sektorių bendradarbiavimą, tobulindama Lietuvos kariuomenės sąveiką su valstybės civiliniais pajėgumais.

11. Lietuva, kaip ir kitos pasaulio valstybės, turinčios puikiai išplėtotą informacinių technologijų ir plačiajuosčių ryšių infrastruktūrą, tampa patraukli ne tik teroristinėms organizacijoms, organizuoto nusikalstamumo grupuotėms, bet ir priešiškoms valstybėms, siekiančioms kibernetinėje erdvėje kelti nacionalines ar tarptautines grėsmes. Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos, Lietuvos Respublikos valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie Lietuvos Respublikos krašto apsaugos ministerijos surinkti duomenys rodo, kad Lietuva nuolat susiduria su įvairaus tipo kibernetiniais išpuoliais ir jų skaičius kasmet didėja.

12. 2016 ir 2017 m. šalyje daugėjo kibernetinių išpuolių prieš viešąjį ir energetikos sektorius, oro uostų, žiniasklaidos tarnybų, taip pat nacionaliniam saugumui svarbių objektų infrastruktūrą. Privačiame ir viešajame sektoriuose kasmet fiksuojama vis daugiau standartinėmis priemonėmis neaptinkamų kibernetinių incidentų, tobulinama elektroninių ryšių tinklų išorinio perimetro kibernetinė žvalgyba, tiriami bandymai sutrikdyti ypatingos svarbos informacinės infrastruktūros objektų veiklą. Lietuvos viešojo sektoriaus ryšių ir informacinės sistemos tebėra prioritetinis kibernetinio šnipinėjimo taikinys, bet taikomasi ir į privataus sektoriaus telekomunikacijų įmones, pramonės objektuose įrengtas industrinių ir

infrastruktūrinių procesų valdymo sistemas, kitas įmones, turinčias strateginę ar svarbią reikšmę nacionaliniam saugumui.

13. Kibernetinių grėsmių paplitimo mastas didelis, todėl kiekvienas subjektas susiduria su situacija, kai reikia spręsti, kiek laiko, pinigų ar kitų išteklių gali prireikti savo ryšių ir informacinių sistemų ar paslaugų apsaugai. Viešojo ir privataus sektoriaus kibernetiniai 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.

14. 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 kibernetinio saugumo grėsmių ir saugumo spragų analizės visapusės integracijos į veiklos rizikos vertinimo procesus, o sparčiai plėtojantis ryšių ir informacinėms sistemoms už kibernetinį saugumą atsakingam personalui pradeda trūkti rizikos vertinimo žinių, gebėjimų ir praktikos.

15. 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:

15.1. nauja redakcija išdėstytos Lietuvos Respublikos kibernetinio saugumo įstatymo nuostatos patobulino kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, atnaujino 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;

15.2. 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, sustiprino Nacionalinį kibernetinio saugumo centrą, kuris tapo vienintele Lietuvos institucija, organizuojančia kibernetinių incidentų valdymą šalyje ir vieno langelio principu teikiančia pagalbą valstybės institucijoms, verslui ir gyventojams.

16. 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.

17. Krašto apsaugos ministerija ir Nacionalinis kibernetinio saugumo centras 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. Po pratybų Krašto apsaugos ministerija kartu su asociacija „Infobalt“ surengė nacionalinę kibernetinio saugumo konferenciją „Cyber Inn“, kurios metu pratybų dalyviai ir svečiai turėjo galimybę pasidalyti savo žiniomis ir patirtimi kibernetinio saugumo srityje, išklausyti Lietuvos ir užsienio šalių ekspertų ir mokslininkų pranešimus apie aktualiausias kibernetinio saugumo užtikrinimo tendencijas, iššūkius ir technologijas.

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.

18. 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 5-uoju 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.

19. **Uždaviniai pirmajam Strategijos tikslui pasiekti:**

19.1. *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 kibernetinio saugumo operacijų centrą ir kompleksinėmis kibernetinio saugumo priemonėmis didinant valstybės valdomo elektroninio ryšių tinklo kibernetinį saugumą, 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.

19.2. *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, atranką, skatinant jomis vadovautis Lietuvoje veikiančias organizacijas ir kibernetinio saugumo paslaugų teikėjus, 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.

19.3. *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.

19.4. *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 Lietuvos Respublikos institucijoms ir įstaigoms.

ANTRASIS SKIRSNIS
NUSIKALTIMAI KIBERNETINĖJE ERDVĖJE

20. **Antrasis Strategijos tikslas** – efektyviau kovoti su nusikaltimais kibernetinėje erdvėje.

21. Kibernetiniai nusikaltimai daro didelį neigiamą poveikį bendrajai Europos Sąjungos skaitmeninei rinkai – nors sunku patikimai įvertinti, įvairių tyrimų duomenimis, pasaulinė kibernetinių nusikaltimų padaryta žala siekia šimtus milijardų eurų per metus. Ne tik finansiniai, bet visi duomenys apskritai labai domina nusikaltėlius, neteisėtų prisijungimų prie ryšių ir informacinių sistemų skaičius nuolat auga, daugėja sukčiavimo ir turto prievartavimo nusikaltimų. Kibernetiniai nusikaltimai yra ypač didelė problema Europos Sąjungos narėms, kuriose interneto infrastruktūra yra gerai išvystyta ir veikia mokėjimo internetu sistemos.

22. Kibernetinių nusikaltimų skaičius Lietuvos Respublikoje, kaip ir visame pasaulyje, nuolat auga. Prognozuojama, kad šis skaičius didės ir toliau, nes daugėja kibernetinių nusikaltimų formų ir krypčių, sparčiai plėtojamos informacinės ir ryšių technologijos (toliau – IRT). Be to, į kibernetinę erdvę persikelia vis daugiau klasikinėmis laikomų nusikalstamumo rūšių. Joms vykdyti ar pėdsakams slėpti pasitelkiami naujausi technologiniai sprendimai, naudojamasi anoniminiame tinkle siūlomomis nusikalstamomis paslaugomis.

Siekiant tinkamai ir efektyviai užkardyti nusikaltimus kibernetinėje erdvėje, peržengiančius valstybių sienas, svarbu plėtoti glaudų tarpvalstybinį bendradarbiavimą ir keitimąsi informacija, 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 kibernetinio saugumo užtikrinimo ir kovos su kibernetiniu nusikalstamumu srityje. Išreikšdama tokią politinę valią, Lietuva ratifikavo Europos Tarybos 2001 m. konvenciją dėl elektroninių nusikaltimų (Budapešto konvencija) ir jos papildomus protokolus ir Europos Tarybos 2007 m. konvenciją dėl vaikų apsaugos nuo seksualinio išnaudojimo ir seksualinės prievartos (Lanzarotės konvencija). Lietuva taip pat perkėlė Europos Parlamento ir Tarybos 2013 m. direktyvą 2013/40/ES dėl atakų prieš informacines sistemas. Įsipareigojimai sėkmingai vykdomi ne tik teisiniu, bet ir praktiniu lygiu, bendradarbiaujant su Tarptautine kriminalinės policijos organizacija (Interpolas) ir Interpolo Pasauliniu inovacijų kompleksu, Europos Sąjungos agentūromis: Europos policijos biuru (Europolas) ir jame veikiančiu Europos kovos su elektroniniu nusikalstamumu centru (EC3), ir Europos teisminio bendradarbiavimo padaliniu (Eurojustas). Taip pat Lietuva dalyvauja Europos teisminio tinklo (EJN) ir Budapešto konvencijos pagrindu įsteigto 24/7 režimu veikiančių kontaktinių punktų kibernetinių nusikaltimų tyrimo srityje tinklo veikloje.

Lietuva, siekdama užkardyti nusikaltimus, susijusius su vaikų seksualiniu išnaudojimu internete, perkėlė Direktyvą 2011/92/ES dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija ir 2012 m. spalio 2 d. ratifikavo Europos Tarybos konvenciją dėl vaikų apsaugos nuo seksualinio išnaudojimo ir seksualinės prievartos.

23. Pastaraisiais metais daugėja nusikalstamų veikų, kai, naudojant kenkimo programinę įrangą ir socialinės inžinerijos priemones, iš nukentėjusiųjų išviliojamos didelės pinigų sumos. Išviliojus prisijungimo prie elektroninės bankininkystės sistemų duomenis, įvykdomos neteisėtos finansinės operacijos. Nusikaltėliai išprovokuoja nukentėjusiuosius pervesti lėšas už tariamas prekes ir paslaugas, į suklastotas sąskaitas faktūras įrašę savo ar savo bendrininkų sąskaitų numerius.

Duomenis šifruojantys kompiuterio virusai, reikalaujantys išpirkos už duomenų iššifravimą, yra viena iš pagrindinių kibernetinių grėsmių, dėl kurios prarandama informacija ir patiriama didelių nuostolių.

Kibernetinius nusikaltimus palengvina ir piktnaudžiavimas anonimiškumą užtikrinančiomis IRT, įskaitant ir anoniminius tinklus bei kriptovaliutas.

24. Nusikaltimams kibernetinėje erdvėje nuolat evoliucionuojant, įgaunant naujų formų, teisėsaugos institucijų personalas, dirbantis kibernetinių nusikaltimų tyrimo ir prevencijos srityje,

turi būti tinkamai pasiruošęs įvertinti esamas ir kylančias grėsmes kibernetinėje erdvėje, identifikuoti kibernetinius nusikaltimus ir efektyviai juos 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.

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

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

25.2. *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 nusikaltimais kibernetinėje erdvėje funkcijų vykdymą ir užtikrinant operatyvesnį tarptautinį bendradarbiavimą tiriant šiuos nusikaltimus, plėtojant teisėsaugos institucijų efektyvų bendradarbiavimą su mokslo, verslo institucijomis ir visuomene kovos su kibernetiniais nusikaltimais srityje.

TREČIASIS SKIRSNIS
KIBERNETINIO SAUGUMO KULTŪRA IR INOVACIJOS

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

27. Kibernetinės grėsmės šiuolaikiniame pasaulyje yra neišvengiamos, nuo jų negalima apsisaugoti net ir taikant visas esamas technines kibernetinio saugumo priemones. Kelti visuomenės kibernetinę kultūrą, supažindinant su kibernetinėmis grėsmėmis, ryšių ir informacinių sistemų saugumo spragomis bei jų daromu poveikiu visuomenei, XXI a. būtina, nes aukštas kibernetinės kultūros lygis padėtų išspręsti daugelį su kibernetiniu saugumu susijusių problemų.

Pasaulinių tyrimų duomenys rodo, kad nuo 50 iki 80 proc. visų kibernetinio saugumo incidentų įvyko todėl, kad pačių nukentėjusių organizacijų darbuotojai nepajėgė atpažinti taikomų socialinės inžinerijos principais paremtų kenkimo atvejų. Kasmet vis daugiau interneto naudotojų patiria nuostolių dėl kibernetinio sukčiavimo, pasireiškiančio užkrėstų laiškų siuntinėjimu ar nuorodų į suklastotas interneto svetaines pateikimu (angl. *phishing*), siekiant išgauti internetinių paskyrų duomenis, finansinę ar kitą svarbią informaciją. Tik 16 proc. interneto vartotojų Lietuvoje mano, kad rizika tapti kibernetinių nusikaltimų aukomis nedidėja (Europos Sąjungos vidurkis 11 proc.), o 48 proc. interneto vartotojų Lietuvoje jaučiasi per mažai informuoti apie kibernetinių nusikaltimų riziką (Europos Sąjungos vidurkis 51 proc.).

28. Lietuvos Respublikos Vyriausybės programoje, kuriai pritarta Lietuvos Respublikos Seimo 2016 m. gruodžio 13 d. nutarimu Nr. XIII-82 „Dėl Lietuvos Respublikos Vyriausybės programos“, švietimas įvardytas kaip svarbiausias prioritetas, valstybės gerovės ir nacionalinio saugumo pagrindas. Kokybiškas ir poreikius atitinkantis kibernetinio saugumo švietimas yra vienas svarbiausių kibernetinės kultūros kėlimo krypčių, mažinančių privataus ir viešojo sektoriaus kibernetinio saugumo riziką.

Pasaulyje atlikta daug tyrimų ir prognozių, jų išvadose konstatuojama esama ir būsima kibernetinio saugumo įgūdžių stoka. Lietuvos Respublikos Vyriausybės programoje numatytas pedagogų rengimo bei kvalifikacijos tobulinimo sistemos pertvarkymas, nes tik talentingi 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. Pažymėtina, kad aukštųjų mokyklų programų, susijusių su kibernetiniu saugumu, nėra daug nei pasaulyje, nei Lietuvoje. Šiuo metu Lietuvoje tik keturi universitetai studentams siūlo kibernetinio saugumo programas, todėl, siekiant užpildyti didėjantį atotrūkį tarp kibernetinio saugumo specialistų paklausos ir pasiūlos, turi būti plėtojamos esamos ir kuriamos naujos studijų programos, skirtos kibernetinio saugumo specialistams rengti.

29. Siekiant apsaugoti valstybės duomenis ir tinklų infrastruktūrą reikia operatyviai reaguojančios ir kvalifikuotos darbo jėgos. Šis poreikis svarbus ir viešajam, ir privačiam sektoriui, ir gyventojams asmeniškai. Valstybė, kurioje trūksta aukštos kvalifikacijos kibernetinio saugumo specialistų, labai pažeidžiama kibernetinio šnipinėjimo, gali sutrikti jos ypatingos svarbos infrastruktūros paslaugų teikimas, pavyzdžiui, sveikatos, energetikos, transporto ir kituose sektoriuose. Privatus sektorius, neturėdamas kvalifikuotų kibernetinio saugumo specialistų, negalėtų identifikuoti sudėtingų kibernetinių incidentų poveikio ir nepajėgtų jo sumažinti, o įmonių išlaidos labai padidėtų. Galiausiai gyventojams, stokojantiems kibernetinio saugumo įgūdžių, gali tekti susidurti su asmens privatumo, finansinio sukčiavimo ir asmens duomenų nutekinimo problemomis.

Asociacijos „Infobalt“ duomenimis, kibernetinio saugumo specialistų Lietuvoje yra nedaug ir šiuo metu darbo rinkoje jų labai trūksta. Valstybės tarnautojams sudaryta galimybė tobulinti savo įgūdžius kibernetinio saugumo srityje, tačiau sprendimus dėl įgūdžių gerinimo priima valstybės ir savivaldybių institucijos ir įstaigos. Nuo 2015 m. didėja valstybės tarnautojų, išklausiusių kursus „Gebėjimų ir įgūdžių elektroninės informacijos saugos (kibernetinio saugumo) srityje tobulinimas“ skaičius. Taip pat nuo 2015 m. labai didėja tokių mokymų poreikis, bet netikrinamos valstybės tarnautojų kibernetinio saugumo žinios nei įsidarbinant (laikant bendrųjų gebėjimų testą), nei vėliau, dirbant. Duomenų, kiek Lietuvos įmonių investuoja į savo darbuotojų kibernetinio saugumo mokymus, nėra, bet akivaizdus ryšių ir informacinių sistemų mokymų trūkumas. Kibernetinio saugumo mokymai ir darbuotojų sertifikavimas turi tapti labiau prieinami darbuotojams tiek privačiame, tiek viešajame sektoriuje.

30. 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 nauja Europos Sąjungos narė, neturinti gilių kibernetinio saugumo mokslinių tyrimų ir mokymo tradicijų – jos sutelktos kitose Europos Sąjungos valstybėse, turi daug galimybių geriau pasinaudoti Europos Sąjungos teikiamomis investicijų į mokslinius tyrimus skatinimo galimybėmis – 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 galimybių įsitraukti į tarptautinius tinklus, ieškant potencialių darbuotojų ir partnerių. Tai paskatintų įmones 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 inovacijoms papildomą postūmį, paskatintų Lietuvos pramonės konkurencingumą ir yra būtinas siekiant atremti šiuolaikines kibernetines grėsmes. Taip pat svarbu skatinti Lietuvos mokslininkų dalyvavimą rengiant tarptautines bendras mokslines publikacijas kibernetinio saugumo srityje, pritraukti daugiau studentų, tiesiogiai dalyvauti aukšto lygio moksliniuose tyrimuose ir eksperimentinės plėtros projektuose kibernetinio saugumo srityje, plėtoti viešojo, privataus sektorių ir mokslo institucijų bendradarbiavimą, padidinti užsienio doktorantų kibernetinio saugumo srityje skaičių.

31. Lietuva, lyginant su kitomis Europos Sąjungos narėmis, padarė didelę pažangą skatindama inovacijas ir gerindama inovacijų ekosistemą, tačiau nuo kitų Europos Sąjungos šalių vis dar atsilieka pagal tokius svarbius inovacijų rodiklius, kaip aukštos pridėtinės vertės eksportas ar eksperimentinės plėtros ir inovacijų išlaidos versle. Lietuvoje dar neatlikti patikimi kibernetinio saugumo rinkos matavimai, bet pripažįstama, kad ši rinka yra auganti, didėja ir kibernetinio saugumo specialistų poreikis. Subalansuotas eksperimentinės plėtros ir inovacijų plėtros poreikis ir pasiūla sudarytų galimybių nuosekliai stiprinti konkurencingos šalies, kuriančios inovatyvius kibernetinio saugumo produktus ir paslaugas, statusą. Šios sinergijos galima siekti jungiant inovacijų iniciatyvas su bendrąja valstybės politika, vykdant Ilgalaikę mokslo, technologijų ir inovacijų plėtros programą.

32. Lietuvoje yra 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 (angl. *FinTech*) įmonių. Ši sritis yra viena iš strateginių Lietuvos banko veiklos krypčių, tad jo veikla vienoje perspektyviausių finansinių technologijų inovacijų – blokų grandinės technologijų (angl. *blockchain*) – srityje veiksmingai prisidės plėtojant finansinių technologijų inovacijas.

33. **Uždaviniai trečiajam Strategijos tikslui pasiekti:**

33.1. *Pirmasis trečiojo tikslo uždavinys* – plėtoti kibernetinio saugumo žinias, mokslinius tyrimus ir didelę pridėtinę vertę kuriančias veiklas. 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,

atliekant mokslinius tyrimus, tobulinant asmenų, dirbančių su jautriais duomenimis, kibernetinio saugumo žinias.

33.2. *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.

33.3. *Trečiasis trečiojo tikslo uždavinys* – skatinti įvairių 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

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

35. Šiuolaikinėse valstybėse su puikiai išplėtota ryšių ir informacinių sistemų infrastruktūra valstybės ir savivaldybių institucijos ir įstaigos nebegali toliau vienos efektyviai kovoti su didelėmis kibernetinėmis grėsmėmis, o ypatingos svarbos informacinės infrastruktūros valdytojai – neretai privataus sektoriaus atstovai – patys ne visada gali suvaldyti kibernetinius incidentus, dažnai peržengiančius organizacijos ribas. Taigi privataus ir viešojo sektorių bendradarbiavimas tampa būtina sąlyga užtikrinant visapusišką kibernetinį saugumą. Efektyvaus privataus ir viešojo sektorių bendradarbiavimo esminė sąlyga – lygiaverčių partnerių abipusis pasitikėjimas ir nauda, todėl privataus ir viešojo sektorių bendradarbiavimas turėtų būti į tai orientuotas.

36. 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.

37. 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.

38. Ryšių ir informacinės sistemos plačiai vartojamos ir jų nauda informacinei visuomenei neabejotina, tačiau didelis ryšių ir informacinių sistemų paplitimas kelia klausimą, kaip efektyviai reaguoti į aptiktas ryšių ir informacinių sistemų saugumo spragas. Ryšių ir informacinių sistemų saugumo spragų ieško asmenys, turintys skirtingų tikslų, tačiau, siekiant atsakingumo atskleidžiant ryšių ir informacinių sistemų saugumo spragas, svarbu sudaryti galimybę saugumo spragą suradusiam ir norinčiam ją ištaisyti asmeniui bendradarbiauti su kibernetinio saugumo subjektais, kurių ryšių ir informacinių sistemų saugumo spraga buvo atskleista. Kibernetinio saugumo subjektai, nustatę ir viešai paskelbę ryšių ir informacinių sistemų saugumo spragų atskleidimo tvarką, visai apsisaugotų nuo žalos arba ją labai sumažintų. Ryšių ir informacinių sistemų saugumo spragų atskleidimo tvarkos nustatymas ir viešas paskelbimas prisidėtų prie valstybės kibernetinio saugumo užtikrinimo ir sudarytų daugiau privataus ir viešojo sektorių bendradarbiavimo galimybių.

39. **Uždaviniai ketvirtajam Strategijos tikslui pasiekti:**

39.1. *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 atsakomybes 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, tobulinant kibernetinio saugumo informacijos mainų platformos veiklos efektyvumą.

39.2. *Antrasis ketvirtojo tikslo uždavinys* – didinti mažų ir vidutinių privataus sektoriaus organizacijų kibernetinio saugumo brandą. Šis uždavinys bus įgyvendinamas skatinant mažas ir vidutines privataus sektoriaus įmones tikrintis kibernetinio saugumo būklę, taisyti kibernetinio saugumo spragas.

39.3. *Trečiasis ketvirtojo tikslo uždavinys* – kurti atsakingą viešojo ir privataus sektoriaus ryšių ir informacinių sistemų saugumo spragų atskleidimo praktiką. Šis uždavinys bus įgyvendinamas inicijuojant atsakingą viešojo ir privataus sektoriaus ryšių ir informacinių sistemų spragų atskleidimo praktiką, nustatant šios srities veiklos principus, metodų, techninių gebėjimų ar kitų priemonių taikymo tvarką.

PENKTASIS SKIRSNIS
TARPTAUTINIS BENDRADARBIAVIMAS

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

41. 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.

42. 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, suderintą NATO ir Europos Sąjungos bendradarbiavimą šioje srityje, siekiant išvengti funkcijų ir veiklų dubliavimosi ir sutapimo. Lietuva stiprins dvišalį politinio ir techninio lygmens bendradarbiavimą, ypač su Jungtinėmis Amerikos Valstijomis.

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

43.1. *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.

43.2. *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.

43.3. *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.

44. Strategijos tikslų pasiekimas vertinamas pagal Strategijos įgyvendinimo vertinimo kriterijus ir jų reikšmes, pateikiamus Strategijos priede.

IV SKYRIUS
STRATEGIJOS ĮGYVENDINIMAS IR ATSAKOMYBĖ

45. Strategijos įgyvendinimą organizuoja Lietuvos Respublikos Vyriausybė, koordinuoja Krašto apsaugos ministerija. Įgyvendinant Strategiją, pagal savo kompetenciją dalyvauja ministerijos, kitos valstybės ir (arba) savivaldybių institucijos, įstaigos ir (arba) organizacijos, nurodytos Strategijos priede (toliau – Strategijos vykdytojai). Nevyriausybinės organizacijos, suinteresuotos visuomeninės grupės ir privataus sektoriaus subjektai gali savo veiksmais prisidėti prie Strategijos vykdymo, jos tikslų ir uždavinių pasiekimo.

46. 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 Nacionaliniam kibernetinio saugumo centrui.

47. 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 remiantis šioje Strategijoje minimu subsidiarumo principu pagal kompetenciją atsako Strategijos vykdytojai.

48. Strategijos įgyvendinimo vertinimo rodikliai ir jų reikšmės nurodyti Strategijos priede. Strategijos įgyvendinimo stebėsenai ir vertinimui taip pat bus naudojami viešai skelbiami Lietuvos statistikos departamento, Eurostato, sociologinių apklausų ir tyrimų duomenys. Strategijos įgyvendinimo rezultatų stebėseną atlieka Krašto apsaugos ministerija, Nacionalinis kibernetinio saugumo centras ir Kibernetinio saugumo taryba.

49. Strategijos vykdytojai, pasibaigus metams, ne vėliau kaip iki kitų metų sausio 15 d. Nacionaliniam kibernetinio saugumo centrui 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. Nacionalinio kibernetinio saugumo centro 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.

50. Gavęs Strategijos 49 punkte nurodytą informaciją, Nacionalinis kibernetinio saugumo centras 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.

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

52. Visa vieša informacija, susijusi su metiniu ir galutiniu Strategijos įgyvendinimo vertinimu, skelbiama Nacionalinio kibernetinio saugumo centro interneto svetainėje.

53. Likus pusei metų iki nustatyto Strategijos įgyvendinimo laikotarpio pabaigos, Nacionalinis kibernetinio saugumo centras parengia ir Krašto apsaugos ministerijai pateikia Strategijos galutinį įgyvendinimo vertinimą, kuris pristatomas Kibernetinio saugumo tarybai ir teikiamas Lietuvos Respublikos Vyriausybei.

Užsienio reikalų ministras
Linas Linkevičius

KAM Administracijos departamento
Dokumentų administravimo skyriaus
vyr. specialistė
Vesta Adomaitienė

Teisės departamento
Įstaigų teisinės priežiūros skyriaus
vedėjas
Antanas Aleknavičius

Krašto apsaugos viceministras
Edvinas Kerza