MYKOLO ROMERIO UNIVERSITETAS

Rekomendacijos Lietuvos Respublikos Kibernetinio saugumo įstatymui

Vilnius, 2017 m.

MYKOLO ROMERIO UNIVERSITETAS

REKOMENDACIJOS LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMUI

Autorių kolektyvas:
dr. Darius Štitilis
dr. Paulius Pakutinskas
dr. Marius Laurinaitis
Inga Malinauskaitė-van de Castel

Mykolo Romerio universitetas
Vilnius, 2017 m. kovo mėn.

MYKOLO ROMERIO UNIVERSITETAS

Rekomendacijos Lietuvos Respublikos Kibernetinio saugumo įstatymui[1]

Kibernetinio saugumo strategijos modelyje (toliau – Modelis) išdėstyta pozicija, argumentai bei įžvalgos leidžia tam tikra apimtimi vertinti esamą Lietuvos teisinį reguliavimą kibernetinio saugumo srityje, kiek šis teisinis reguliavimas atitinka autorių sukurtą Modelį. Autorių atlikti tyrimai leidžia pateikti teisinio reguliavimo tobulinimo įžvalgas įvertinus Europos Sąjungos bei NATO valstybių gerąsias patirtis. Toliau pateikiamos rekomendacijos pagrindiniam Lietuvos Respublikos teisės aktui kibernetinio saugumo srityje – Lietuvos Respublikos Kibernetinio saugumo įstatymui (toliau – Įstatymui) patobulinti.

Dėl sąvokų

Visų pirma, paminėtina, kad tiriant sąvokas, buvo naudojamas lingvistinis metodas. Šis metodas buvo reikšmingas atskleidžiant sąvokų turinį, taip pat tiriant terminijos naujadarus. Atliekant lyginamąjį Europos Sąjungos ir NATO valstybių nacionalinių kibernetinio saugumo strategijų tyrimą, buvo susidurta su regioniniuose bei atskirų valstybių dokumentuose naudojamomis skirtingomis sąvokomis, todėl sąvokų interpretavimas taip pat buvo svarbus kuriant Lietuvos nacionalinės kibernetinio saugumo strategijos modelį.

Antra, pažymėtina, kad sąvokos svarbios ne tik nacionalinės kibernetinio saugumo strategijos kontekste. Sąvokos nacionalinėje kibernetinio saugumo strategijoje turi sukurti pagrindą vienodam ir sisteminiam sąvokų kibernetinio saugumo srityje naudojimui kituose valstybės dokumentuose, pradedant LR kibernetinio saugumo įstatymu ir baigiant lydimaisiais teisės aktais. Nacionalinėje kibernetinio saugumo strategijoje pateikiamos sąvokos turi būti pagrindu ir pavyzdžiu formuojant ir naudojant sąvokas kituose dokumentuose. Tik taip galima užtikrinti nuoseklų sąvokų panaudojimą, išvengti prieštaravimų sąvokose bei išvengti problemų, kurios gali kilti dėl netinkamų, nekokybiškų ar prieštaraujančių sąvokų naudojimo. Pažymėtina, kad sąvokos kibernetinio saugumo srityje turėtų būti neutralios, atitikti technologinio neutralumo, funkcinio ekvivalentiškumo ir kitus susijusius principus, būti neperkrautos gramatiškai ir pertekline informacija.

Toliau pateikiami autorių pastebėjimai ir pasiūlymai dėl Įstatyme egzistuojančių atitinkamų sąvokų:

Kibernetinė erdvė *– aplinka, kurioje pavieniuose kompiuteriuose ar kitoje informacinėje ir ryšių technologijų įrangoje sukuriama elektroninė informacija ir (arba) perduodama per elektroninių ryšių tinklu sujungtus kompiuterius ar kitą informacinių ir ryšių technologijų įrangą.*

Siūloma keisti šią sąvoką. Erdvė gali būti fizinė, elektroninė, todėl keistina į technologiškai neutralią ir gramatiškai teisingą:

Elektroninė erdvė *– aplinka kur galimas efektyvus veiksmas per atstumą pasinaudojant informacinėmis technologijomis.*

1 Šios Rekomendacijos parengtos kaip mokslinio projekto „ES ir NATO valstybių kibernetinio saugumo strategijų normų analizė ir adaptavimas Lietuvos situacijai - Lietuvos kibernetinio saugumo strategijos modelis, Nr. MIP-099/2015, rezultatų dalis.

Pastaba: autoriai pastebi, kad sąvokos „kibernetinė erdvė“ ir „elektroninė erdvė“ Lietuvos teisės aktuose ir kituose dokumentuose naudojamos kaip sinonimai. Autoriai siūlo svarstyti šį kelių sąvokų naudojimo klausimą ir spręsti dėl vienos sąvokos naudojimo terminologijoje, susijusioje su kibernetiniu saugumu. Nuo sąvokos pasirinkimo nei naudojimo taip pat priklausys ir kitos sąvokos (pvz., pasirinkus sąvoką „elektroninė erdvė“, reikėtų svarstyti ir tokias sąvokas, kaip „kibernetinis incidentas“ bei kt. Šia pastaba autoriai iškelia pačią problemą, tačiau toliau rekomendacijose šiuo aspektu sąvokos nekeičiamos. Iškeltą problemą paliekama suinteresuotoms šalims spręsti ateityje, nes problema yra kompleksinė, apimanti ne vieną teisės aktą ir / ar dokumentą.

Kibernetinis incidentas *– įvykis ar veika, kuri sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos, sutrikdyti ar pakeisti, įskaitant valdymo perėmimą, informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims.*

Siūloma keisti šią gramatiškai sudėtingą sąvoką, kuri perkrauta nereikalingais atskirų teisės pažeidimų el. erdvėje būdais. Lietuvos Respublikos baudžiamasis kodeksas atskirai nurodo tokius teisės pažeidimus: nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui. Į šią sąvoką nereikėtų perkelti atskirų pažeidimų turinio, jei tai neturės jokios reikšmės identifikuojant atitinkamą reiškinį? Siūloma keisti į tiesiog:

Kibernetinis incidentas *– incidentas – įvykis, turintis faktinį neigiamą poveikį elektroninių duomenų, tinklų ir informacinių sistemų saugumui.*

Taip pat siūloma įtraukti šią sąvoką:

Incidentų valdymas *– visos procedūros, padedančios nustatyti, ištirti bei suvaldyti incidentą ir į jį reaguoti.*

Kibernetinis saugumas *– visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti.*

Siūlomas keisti į praktinį saugumo apibrėžimą, nevartojant žodžių išvengti ir t.t.:

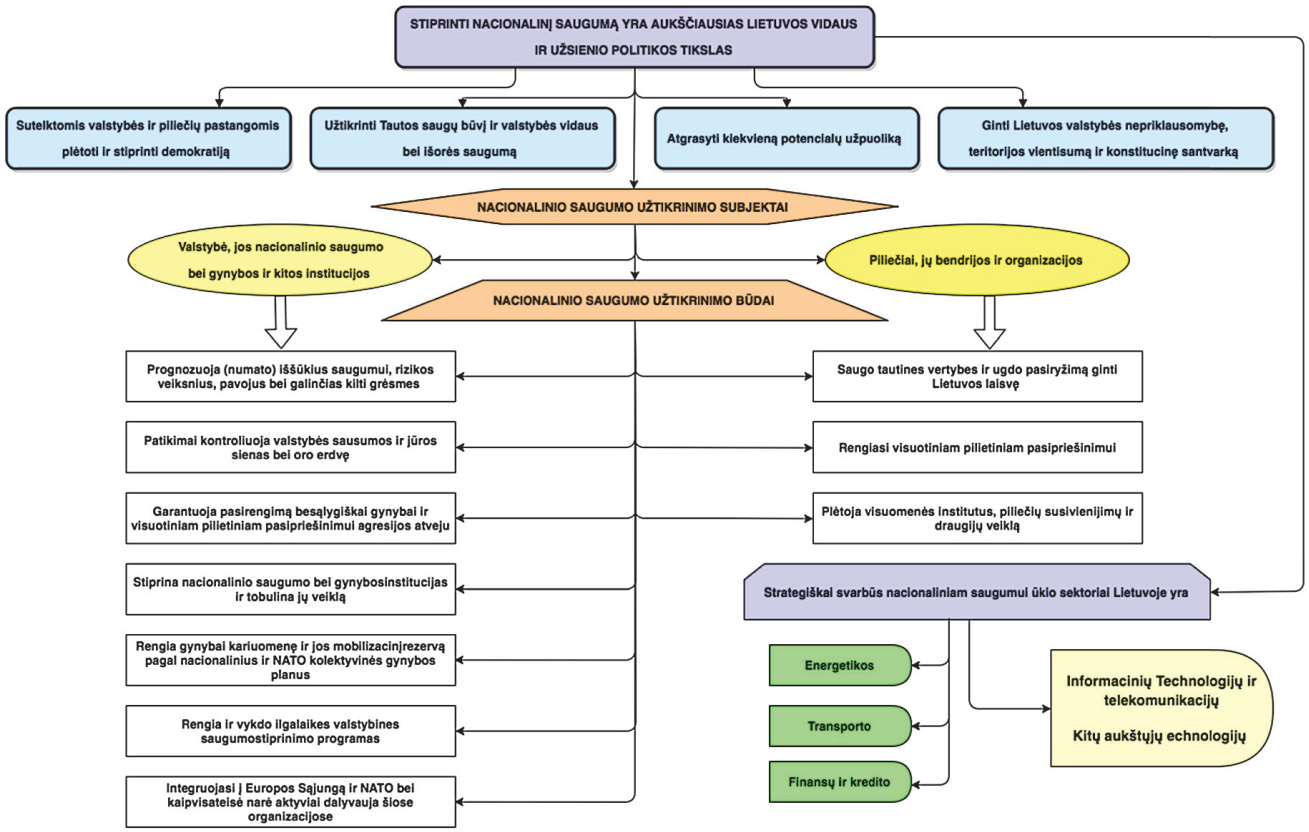
Tinklų ir informacinių sistemų saugumas *– tinklų ir informacinių sistemų pajėgumas tam tikru patikimumo lygiu išlikti atsparus bet kuriems veiksmams, keliantiems pavojų saugomų, perduodamų ar tvarkomų duomenų, arba atitinkamų teikiamų ar per tas tinklų ir informacines sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui.*

Jei Įstatyme bus įvedami papildomi institutai, kaip siūloma šiose rekomendacijose, papildomai reikėtų svarstyti ir naujų sąvokų įvedimą:

- „Pagrindinė atsakinga institucija“;
- „Kibernetinio saugumo švietimo programa“;
- „Kibernetinio saugumo kultūra“;
- „Kibernetinė gynyba“;
- „Tarptautinis bendradarbiavimas“.

Dėl visuomenės ir piliečių įsitraukimo

Nagrinėjant kitų valstybių kibernetinio saugumo strategijas buvo pastebėta, kad daugelio šalių strategijose yra minimi valstybių piliečiai bei visuomenė kaip kibernetinio saugumo dalyviai arba subjektai. Įstatymo 1 straipsnio 2 dalyje tarp vardijamų kibernetinio saugumo dalyvių, t.y. kam yra skiriamas Įstatymas, rekomenduojama papildyti dalyvių sąrašą „visuomene“ arba „piliečiais“, tuo priartinant Įstatymo nuostatas prie kiekvieno Lietuvos Respublikos visuomenės nario / piliečio. Tai sistemiškai atspindėtų ir Lietuvos Respublikos nacionalinio saugumo įstatyme numatytą visuomenės bei piliečio vaidmenį, kurį galima pavaizduoti šioje schemoje žemiau:



Ši aukščiau pateikta schema patvirtina, kad reikėtų peržiūrėti piliečių ir kitų subjektų įtraukimą į procesus ir pagal galimybes Įstatyme įtvirtinti teises bei pareigas. Tai galėtų apimti ir tokias sritis, kaip kibernetinio saugumo higiena bei pan.

Jei piliečių ir visuomenės įtraukimas, reglamentuojamas Nacionalinio saugumo pagrindų įstatyme, panašūs principai turėtų būti įtvirtinami ir specialiame kibernetinio saugumo reguliavime, įstatyme ir lydimuosiuose teisės aktuose.

Dėl Įstatyme numatytų principų

Įstatymo 3 straipsnyje paminėta, kad Kibernetinis saugumas grindžiamas bendraisiais teisės principais, elektroninių ryšių veiklos reguliavimo principais ir šiais kibernetinio saugumo principais: kibernetinės erdvės nediskriminavimo, kibernetinio saugumo proporcingumo ir viešojo intereso viršenybės. Taikant kibernetinį saugumą reglamentuojančias teisės normas, turi būti tinkamai atsižvelgiama į visus šiuos nurodytus principus. Šie principai turi būti derinami tarpusavyje nė vienam iš jų iš anksto nesuteikiant pirmenybės.

Kibernetinio saugumo principai Įstatyme atskleisti sistemiškai, pabrėžti bendrieji teisės principai, elektroninių ryšių veiklos reguliavimo principai, išskirti specifiniai kibernetinio saugumo principai. Įstatymas išsamiau galėtų akcentuoti pagrindinių žmogaus teisių ir laisvių apsaugos svarbą – vertybes, kurių gynimui ir apsaugai turėtų tarnauti šis įstatymas. Minėtos vertybės ir principai nenustos savo svarbos, jei nebus paminėti Įstatyme, tačiau, siekiant visų rūšių saugumo, reikia prisiminti, kad negalima peržengti atitinkamų vertybių ir žmogaus teisių. Įstatyme apibrėžtų kibernetinio saugumo principų išskirtinumas ir specifiškumas gali būti diskutuotinas, nes kibernetinės erdvės nediskriminavimo principas nėra specifinis tik šios srities principas, jis įvardinamas bei svarbus ir kitose elektroninės erdvės srityse.

Atskirai verta akcentuoti proporcingumo principą.

Dėl viešojo intereso viršenybės principo išskyrimo pažymėtina, kad valstybė turėtų skatinti ne tik abstraktaus viešojo intereso apsaugą, bet ir bendradarbiavimo principą, kuris apimtų ne tik tarptautinį, bet ir tarpinstitucinį bei privataus ir viešojo sektorių bendradarbiavimą.

Taip pat, labai svarbu paminėti asmeninės atsakomybės principą, kuris sudaro prielaidas ir viešojo intereso apsaugai. Visuotinės gynybos principas įtvirtintas fizinės gynybos reguliavime yra svarbus ir kibernetinėje saugoje, nes netinkamas, neatsakingas elgesys, priemonės, kibernetinis neraštingumas gali skatinti kibernetinius incidentus. Kibernetinio saugumo, kaip integralios nacionalinio saugumo dalies, principas svarbus ne tik nagrinėjamame Įstatyme, bet ir nacionalinį saugumą reguliuojančiose normose.

Dėl kibernetinės gynybos

Atkreiptinas dėmesys, kad vienas iš 2013 m. ES kibernetinio saugumo strategijos tikslų – sukurti kibernetinės gynybos politiką ir pajėgumus, susijusius su bendra saugumo ir gynybos politika. Lietuvos Respublikos nacionalinio saugumo pagrindų įstatyme Lietuvos gynybinė galia grindžiama tautos apsisprendimu ir pasiryžimu priešintis kiekvienam užpuolikui. Pagal elektroninės erdvės nediskriminavimo ir funkcinio ekvivalentiškumo principus, kibernetinė gynyba turėtų būti traktuojama plačiau nei tik ypatingos svarbos infrastruktūros ar valstybės informacinių išteklių apsauga.

Įstatyme patartina įvesti nuostatas dėl kibernetinės gynybos. Kibernetinė gynyba šiuo metu Įstatyme iš viso neaptarta. Tam tikru aspektu, kiek tai susiję su kritine infrastruktūra ar valstybės informaciniais ištekliais, kibernetinės gynybos elementai yra reglamentuojami lydimuosiuose teisės aktuose. Tačiau Įstatyme būtinos nuostatos ne tik dėl gynybos atitinkamuose sektoriuose, bet dėl kibernetinės gynybos visos valstybės mastu, įtraukiant visas galimas suinteresuotas šalis. Todėl patartina atitinkamai peržiūrėti ir papildyti Įstatymą.

Dėl bendradarbiavimo

Įstatyme reikėtų išsamiau reglamentuoti bendradarbiavimą įvairiais lygiais, tiek valstybės viduje tarp skirtingų subjektų, tiek išorėje, t.y. su tarptautiniais subjektais. Kaip jau minėta aukščiau, bendradarbiavimas, turint omenyje grėsmes, kurioms neegzistuoja sienos, yra vienas iš pagrindinių elementų kovojant su kibernetinėmis grėsmėmis.

Dėl institucinės sistemos

Vienas iš Modelyje pastebėtų aspektų yra institucinės sistemos, atsakingos už kibernetinį saugumą Lietuvoje, netikslumas, neaiškiai išdėstytos institucijų funkcijos ir atsakomybės, nėra aiškios pagrindinės institucijos, kuri prisiimtų atsakomybę už kibernetinio saugumo valdymą bei prevenciją.

Nors įstatyme yra išskirta institucinė kibernetinio saugumo sistema, paminėtina, kad Nacionalinis kibernetinio saugumo centras yra Lietuvos Respublikos krašto apsaugos ministerijos struktūrinis padalinys ir nėra *de jure* savarankiška institucija. Tokia praktika yra ydinga dėl kelių priežasčių:

- Krašto apsaugos ministerija yra ne tik kibernetinio saugumo politiką formuojanti, jos įgyvendinimą organizuojanti, kontroliuojanti bei koordinuojanti institucija, bet taip pat ir viešojo administravimo subjektas, privalantis vykdyti įpareigojimus kibernetinio saugumo srityje, taip pat institucija. Tokios institucijos struktūrinis padalinys – Nacionalinis kibernetinio saugumo centras – negali kontroliuoti, kaip institucija laikosi kibernetinio saugumo reikalavimų, t.y. institucija negali kontroliuoti savęs, o Krašto apsaugos ministrui negali vadovauti vieno iš šios ministerijos struktūrinių padalinių vadovas. Turi būti nustatytas efektyvus kontrolės mechanizmas;
- Nacionaliniam kibernetinio saugumo centrui esant struktūriniam Krašto apsaugos ministerijos padaliniui, nėra atskirtos politikos formavimo ir kontrolės mechanizmai, funkcijos. Tokių funkcijų atskyrimas akcentuojamas pažangiausiose (kibernetinio saugumo užtikrinimo prasme) valstybėse, tokiose, kaip Vokietija, Suomija ir kt.;
- Nacionalinio kibernetinio saugumo centro funkcijas vykdant vienam iš ministerijų struktūrinių padalinių, gali atsirasti veiklos koordinavimo su kitomis institucijomis ir nurodymų vykdymo problemos. Kaip rodo praktika, Lietuvoje šiuo metu ypač stinga tarpinstitucinio bendradarbiavimo, o struktūrinis vienos iš ministerijų padalinys iš esmės nėra pajėgus spręsti tokias problemas. Taip pat, struktūrinis ministerijos padalinys iš esmės negali nulemti kitų ministerijų resursų panaudojimo bendrai sprendžiant kibernetinio saugumo klausimus.

Lietuvoje reikėtų įtvirtinti savarankišką instituciją. Kaip Lietuvoje veikiantis geras pavyzdys galėtų būti Valstybinė duomenų apsaugos inspekcija, kuri šiuo metu atskaitinga Lietuvos Respublikos Vyriausybei. Įstatymo 1 straipsnio 1 dalyje būtų tikslinga papildyti nauja sąvoka „pagrindinė atsakinga už kibernetinį saugumą instituciją“.

Įstatymo 4 straipsnyje rekomenduotina aiškiau ir konkrečiau suformuluoti institucijų funkcijas. Be to, rekomenduojama papildyti 4 str. 2 dalyje „pagrindine atsakinga institucija“ bei jos nustatoma funkcija ar funkcijomis, suderintomis su kitų institucijų funkcijomis. Atitinkamai, didžiąją dalį „pagrindinės institucijos“ funkcijų būtų perkeliama iš šiuo metu įvardintų Nacionalinio kibernetinio saugumo centro funkcijų.

Rekomenduojama atitinkamai tobulinti bei tikslinti Įstatymo 6 ir 10 straipsnius patikslinant bei aiškiau nustatant tiek Krašto apsaugos ministerijos, tiek Nacionalinio kibernetinio saugumo centro statusą bei vykdomas funkcijas. Rekomenduotina jas suderinti bei išgryninti.

Dėl švietimo ir kibernetinio saugumo kultūros

Kuriant Modelį, vienas iš keliamų klausimų buvo, ar ir kaip visuomenė žinos apie priemones kibernetiniam saugumui užtikrinti. Kitas svarbus aspektas – kaip bus vykdomas visuotinės gynybos principas, kuris skelbia visuomenės ir kiekvieno visuomenės nario pareigą gynybai. Įvairūs tyrimai rodo, kad visuomenės žinios dėl kibernetinio saugumo priemonių taikymo yra menkos ir tai gali neigiamai paveikti kibernetinio saugumo situaciją bendrąja prasme. Tai suponuoja, kad visuomenę reikia šviesti.

Šiuo metu Įstatyme švietimo klausimai išvis neaptariami ir nereglamentuojami. Įstatyme turėtų būti įtvirtinama bendra pareiga šviesti visuomenę įvairiais lygiais. Bendroji norma dėl švietimo įtvirtintų taisyklę, pabrėžiančią švietimo svarbą. Tačiau švietimas neturėtų būti susijęs tik su Švietimo ir mokslo ministerijos funkcijomis. Turėtų būti įtvirtinamos bendrosios pareigos švietimu rūpintis visiems subjektams. Iš esmės, reikėtų siekti, kad švietimas kibernetinio saugumo srityje būtų pradedamas nuo vaikų darželių, mokyklų pirmųjų klasių. Taip būtų formuojami socialinio elgesio elektroninėje erdvėje įgūdžiai, kibernetinių grėsmių suvokimas.

Taigi, Įstatyme reikėtų skirti atskirą dėmesį švietimui.