MYKOLO ROMERIO UNIVERSITETO

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

GIEDRĖ ŪDRAITĖ

Kibernetinio saugumo valdymo programa

KIBERNETINIO SAUGUMO NACIONALINIŲ STRATEGIJŲ KŪRIMO IR DIEGIMO YPATUMAI: PASAULIO ŠALIŲ ANALIZĖ

Magistro baigiamasis darbas

Darbo vadovas –

Prof. Dr. Tadas Limba

Vilnius, 2021

TURINYS

ĮVADAS

Temos aktualumas ir naujumas. Informacinių technologijų galimybės nuolat plečiasi, technologijos skverbiasi į pačias įvairiausias žmonių veiklos sritis, tačiau paraleliai auga kibernetinių incidentų skaičius, incidentai sudėtingėja. Nepaisant to, kad Jungtinių Tautų Tarptautinės telekomunikacijų sąjungos, įvertinusios valstybių pajėgumus kibernetinio saugumo srityje, paskelbtame Globaliajame kibernetinio saugumo indekse Lietuva iš 57-tos vietos 2017 m. pakilo į 4-ąją vietą 2019 m., atsipalaiduoti nereikėtų. 2020 m. kibernetinių incidentų padaugėjo 25 procentais, o su kenkimo programinės įrangos platinimu susijusių incidentų skaičius išaugo net 49 procentais. Lietuvos Respublikos krašto apsaugos ministerijos 2020 m. Nacionalinės kibernetinio saugumo būklės ataskaitos duomenimis, 2019 m. užregistruotas 3241 kibernetinis incidentas, o 2020 m. – 4330 incidentų. Kibernetinių incidentų skaičiaus augimą 2020 m. įtakojo ir COVID-19 pandemijos suvaldymui skirti apribojimai, dėl kurių daugelio žmonių darbas, mokymasis ir laisvalaikis persikėlė į elektroninę erdvę. Itin išaugus įvairių informacinės visuomenės paslaugų poreikiui, tuo pasinaudojo ir piktavaliai.

Kibernetinės atakos ypač pavojingos valstybėms, turinčioms gerai išvystytus kompiuterių tinklus. Tokioms valstybėms priskirtina ir Lietuva, kurioje informacinių technologijų plačiajuostis optinis tinklas apima beveik 98 proc. teritorijos. Per pastaruosius kelerius metus kibernetinės atakos buvo nukreiptos į Lietuvos Respublikos Prezidentūrą, Seimą, Užsienio reikalų ministeriją, Krašto apsaugos ministeriją, Vidaus reikalų ministeriją, Teisingumo ministeriją. Atakas taip pat patyrė Valstybinė mokesčių inspekcija, kai kurios žiniasklaidos priemonės, komunalines paslaugas teikiančios įmonės. Atakos nukreipiamos ir prieš pačias įvairiausias socialines platformas, gydymo ir sveikatinimo paslaugas teikiančias įmones, tvarkančias itin jautrius asmens duomenis, kurių praradimas ar atskleidimas gali sukelti neatitaisomą žalą.

Kiekviena valstybė privalo prisiimti įsipareigojimus užkirsti kelią kenkėjiškoms kibernetinėms atakoms, todėl būtina sukurti nacionalinius kibernetinio saugumo pajėgumus (įsteigti institucijas, priimti teisės aktus, reglamentuoti atitinkamas procedūras) ir prisiimti būtiniausius įsipareigojimus, siekiant užtikrinti nacionalinės kibernetinės erdvės saugumą. Vienas iš pagrindinių dokumentų, kuriuo siekiama šio tikslo įgyvendinimo – valstybės nacionalinė kibernetinio saugumo strategija, nustatanti tiek esminius kibernetinio saugumo užtikrinimo principus, tikslus, prioritetus, tiek detalius kibernetinio saugumo priemonių įgyvendinimo planus.

Valstybių nacionalinės kibernetinio saugumo strategijos skiriasi tiek turiniu, tiek tęstinumu. Nemaža dalis valstybių nurodo tik strategijų priėmimo metus, o strategijos galiojimas apsprendžiamas naujosios strategijos. Kita dalis valstybių nurodo ir galiojimą, kuris siekia 2 – 5 metus. Strategijų planavimas keleriems metams į priekį nebūtinai reiškia jose numatytų priemonių tęstinumą – dalies

priemonių atsisakoma kaip nepasiteisinusių, jos keičiamos naujomis, progresyviomis priemonėmis. Lietuvos Nacionalinė kibernetinio saugumo strategija buvo patvirtinta 2018 m., joje numatytos priemonės turi būti įgyvendintos iki 2023 m.

Mokslinė problema: mokslo šaltiniuose kibernetinio saugumo strategijų kūrimo ir diegimo procesų problematika nepakankamai išanalizuota. Mokslinės analizės ir praktinių rekomendacijų trūkumas apsunkina efektyvių ir inovatyvių kibernetinės erdvės saugumą įgyvendinti padedančių priemonių diegimą.

Tyrimo objektas: nacionalinių kibernetinio saugumo strategijų kūrimas ir diegimas.

Tyrimo tikslas: išanalizuoti pasirinktų valstybių kibernetinio saugumo strategijas, jose numatytus pagrindinius principus ir priemones bei pritaikyti juos kuriant Lietuvos kibernetinio saugumo strategijos modelį.

Uždaviniai:

1. Atlikti pasirinktų užsienio valstybių kibernetinio saugumo strategijų kūrimo ir diegimo procesų teorinę analizę;
2. Išanalizuoti pasirinktų užsienio valstybių kibernetinio saugumo strategijų turinį, nustatyti strategijų privalumus ir trūkumus;
3. Išsiaiškinti 2018–2023 m. Lietuvos kibernetinio saugumo strategijos teisines spragas ir problemas, įgyvendinant joje numatytas priemones;
4. Pasirinktų valstybių gerosios praktikos analizės pagrindu pasiūlyti kibernetinio saugumo strategijos modelį.

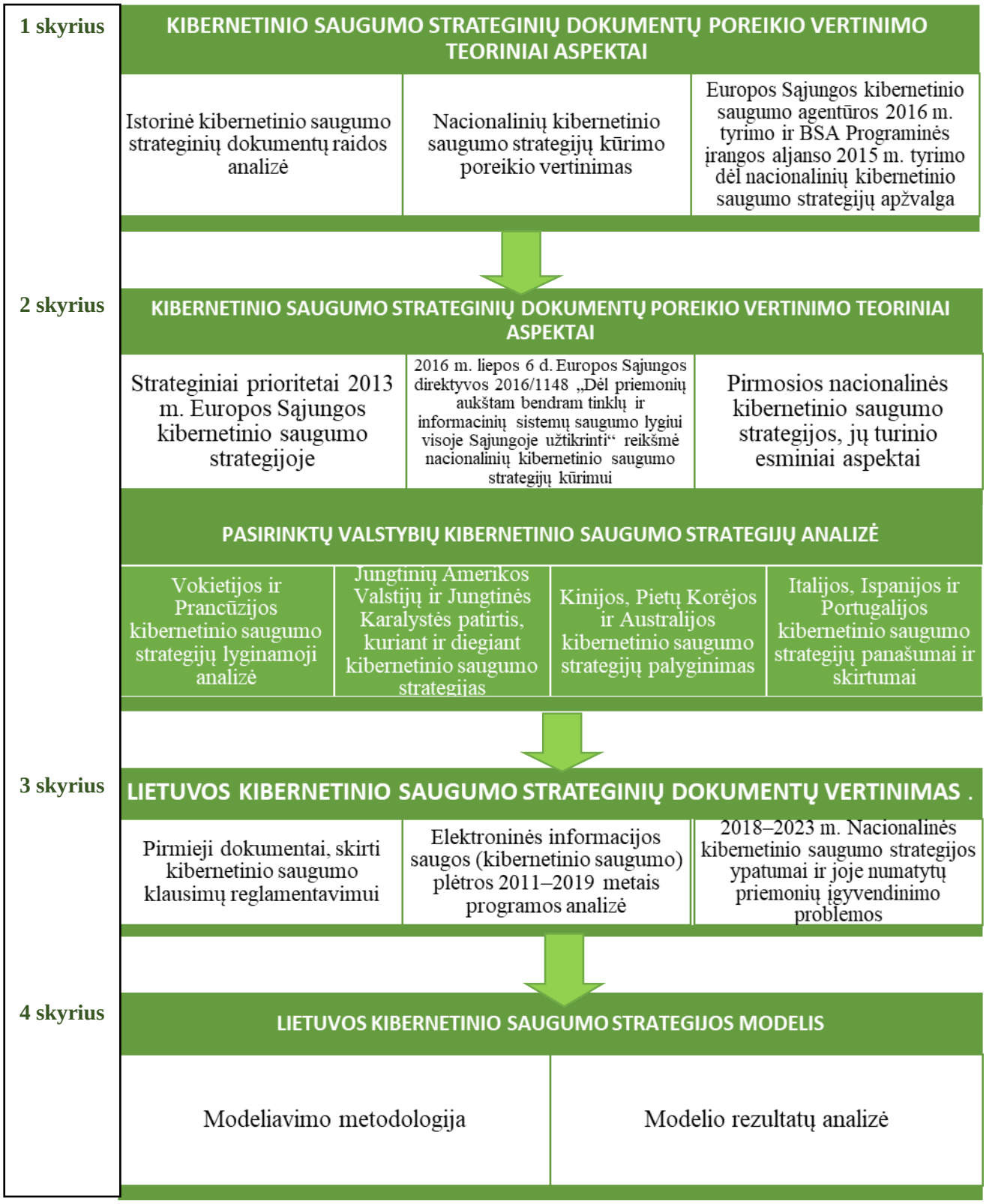
Tyrimo metodai ir šaltiniai. Darbe atlikta mokslinės literatūros analizė kibernetinio saugumo srityje, koncentruojantis į daugiausiai dėmesio šiai sričiai skyrusių ekspertų – prof. dr. D. Štitilio, dr. M. Laurinaičio ir prof. dr. P. Pakutinsko mokslines publikacijas, detaliai išnagrinėti pasirinktų užsienio valstybių (Vokietijos, Prancūzijos, Jungtinių Amerikos Valstijų, Jungtinės Karalystės, Kinijos, Pietų Korėjos, Australijos, Ispanijos, Italijos, Portugalijos) strateginiai dokumentai. Taip pat apžvelgti Europos Sąjungos strateginiai dokumentai, išsamiai analizuotas Lietuvos Respublikos teisės aktų, reglamentuojančių kibernetinio saugumo klausimus, turinys. Remiantis atvejo analizės metodu, išanalizuoti pasirinktų valstybių kibernetinio saugumo klausimus reglamentuojantys dokumentai, aptarti jų privalumai ir trūkumai. Darbe taip pat naudoti kiekybiniai ir kokybiniai tyrimo metodai, analizuojant tyrimų dėl pasirinktų valstybių kibernetinio saugumo strategijose numatytų priemonių įgyvendinimo duomenis.

Darbo struktūra. Magistro baigiamąjį darbą sudaro keturi pagrindiniai skyriai. Pirmajame skyriuje analizuojami nacionalinių kibernetinio saugumo strategijų poreikio kilimo istoriniai aspektai, pirmieji valstybių žingsniai kuriant ir diegiant savo nacionalines kibernetinio saugumo strategijas. Antrasis skyrius skirtas pasaulinės patirties kuriant ir diegiant kibernetinio saugumo strategijas

apžvalgai, analizuojamas pasirinktų užsienio valstybių kibernetinio saugumo strategijų turinys, aptariamos jų įgyvendinimo problemos. Taip pat šiame skyriuje aptariama 2013 m. Europos Sąjungos kibernetinio saugumo strategijos ir 2016 m. liepos 6 d. Europos Sąjungos direktyvos 2016/1148 „Dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti“ reikšmė nacionalinių kibernetinio saugumo strategijų kūrimui. Trečiajame skyriuje analizuojama Lietuvos patirtis, kuriant ir diegiant kibernetinio saugumo strategijas, nagrinėjamas 2018 m. patvirtintos Nacionalinės kibernetinio saugumo strategijos turinys, joje numatytų priemonių įgyvendinimo perspektyvos. Ketvirtajame skyriuje analizuojamas Lietuvos ekspertų 2017 m. pateiktas Lietuvos kibernetinio saugumo strategijos modelis, pateikiamas kibernetinio saugumo strategijos modelio pavyzdys, parengtas remiantis pasirinktų užsienio valstybių gerąja praktika.

Teorinis ir praktinis reikšmingumas. Priėmus Kibernetinio saugumo įstatymą, nustatantį institucijas, atsakingas už kibernetinio saugumo politikos įgyvendinimą, jų kompetenciją, funkcijas, teises bei pareigas, įsteigus Kibernetinio saugumo centrą ir patvirtinus Lietuvos Nacionalinę kibernetinio saugumo strategiją, kibernetinio saugumo įgyvendinimo situacija Lietuvoje ženkliai pagerėjo, tačiau tikėtis stabilumo elektroninėje erdvėje nevertėtų. Ne visos Nacionalinėje kibernetinio saugumo strategijoje numatytos priemonės realiai įgyvendinamos, pati strategija taip pat nėra tobula, kaip ir kitų valstybių nacionalinės kibernetinio saugumo strategijos. Dėl šios priežasties būtina nuolat ir nuosekliai tobulinti kibernetinį saugumą reglamentuojančius teisės aktus, atnaujinti nacionalinėje kibernetinio saugumo strategijoje numatytas priemones, skirtas kibernetiniam saugumui užtikrinti, stiprinti jas įgyvendinančių subjektų bendradarbiavimą.

Šis darbas atskleis egzistuojančias kibernetinio saugumo nacionalinių strategijų kūrimo ir įgyvendinimo problemas, jame bus pateikti praktiniai siūlymai naujos Lietuvos kibernetinio saugumo strategijos rengimui bei kibernetinio saugumo strategijos modelis.



1 pav. Magistro baigiamojo darbo struktūros loginė schema

1. KIBERNETINIO SAUGUMO STRATEGINIŲ DOKUMENTŲ POREIKIO VERTINIMO TEORINIAI ASPEKTAI

1.1 Istorinė kibernetinio saugumo strateginių dokumentų raidos analizė

Pasaulio bendruomenei skiriant vis daugiau laiko ir pastangų kibernetinio saugumo užtikrinimui, informacinių technologijų eksperto G. Meškausko 2015 m. išsakyta nuomonė apie tai, kad „kibernetinis saugumas yra tokio lygio, koks buvo transporto eismo saugumas vos tik jam atsiradus“[1], šiandien gali atrodyti pernelyg radikali. Vis dėlto, kibernetinio saugumo užtikrinimo aktualumas nemažėja. Be informacinių technologijų, informacinių sistemų, interneto prieigos daugelis visuomenėje vykstančių procesų sunkiai įsivaizduojami, o kibernetinių incidentų pasekmės tampa globalios ir retai būna susijusios tik žala atskiriems individams ar organizacijoms.

Prieš pradedant kibernetinio saugumo klausimus reglamentuojančių dokumentų analizę, būtina aptarti ir kibernetinio saugumo sąvoką, nes ji šiame darbe – kertinė. Lietuvos Respublikos kibernetinio saugumo įstatymo 2 straipsnio 10 dalyje pateikiamas toks kibernetinio saugumo apibrėžimas: tai „*visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą*“.

Mokslinėje literatūroje galime rasti tiek sudėtingesnių (*procesų, susijusių su kibernetinėmis grėsmėmis, identifikavimas ir sąnaudomis pagrįstų kontrpriemonių taikymas, kūrimas ir palaikymas*), tiek nesunkiai suvokiamų (*apsauga nuo netinkamo interneto infrastruktūros naudojimo ir jos žlugdymo*[2]; *priemonės, skirtos kompiuterio ar kompiuterių tinklo apsaugai nuo neleistinos prieigos ar atakos*[3]*)* kibernetinio saugumo sąvokų.

Pasaulio valstybių kibernetinio saugumo strategijose pateikiamos sąvokos skiriasi. Pvz., Prancūzijoje kibernetinis saugumas apibrėžiamas kaip tam tikra informacijos sistema, leidžianti pasipriešinti įvykiams, kurie gali pakenkti prieinamumui, vientisumui ar saugumui duomenų, saugomų, apdorojamų ar perduodamų tarp informacijos ir ryšių sistemų. Naujojoje Zelandijoje orientuojamasi į veikas, saugančias kibernetinę erdvę nuo įsilaužimų, leidžiančias išlaikyti

[1] G. Meškauskas „Nepatingėkite užduoti kontrolinio klausimo“. 2015 m. liepos 3 d. publikacija internete: G. Meškauskas: „Nepatingėkite užduoti kontrolinio klausimo“ - Bernardinai.lt

[2] Shoemaker, D. and Conklin, A. 2012. Cybersecurity: the Essential body of knowledge. Course technology, p. 11.

[3] E. F. Chamorro, J. R. C. Fernandez, R. M. Lopez, S. L. Fernandez „National Cyber Security, a commitment for everybody“, 2012. P. 13.

informacijos konfidencialumą, vientisumą ir prieinamumą ir identifikuojančias įsilaužimus ir incidentus[4]. Rusijoje kibernetinis saugumas suvokiamas kaip tam tikra informacinių sistemų būklė, o pati informacija traktuojama tiek kaip vertybė, tiek kaip ginklas[5].

Įvertinus įvairias kibernetinio saugumo sąvokas, galima teigti, kad daugelyje jų akcentuojami **veiksmai** (atitinkamų priemonių, jų plano sukūrimas, žalingų procesų identifikavimas, apsaugos (saugumo lygio) užtikrinimas), kuriais siekiama **užtikrinti saugumą** (atsparumą, pajėgumą pasipriešinti atakoms) **kibernetinėje erdvėje** (tinklų ir informacinėse sistemose, interneto infrastruktūrose).

Pirmasis tarptautinis dokumentas, skirtas spręsti nusikalstamų veikų elektroninėje erdvėje problemas, yra 2001 m. lapkričio 23 d. Budapešte pasirašyta Konvencija dėl elektroninių nusikaltimų (Budapešto konvencija[6]). Pagrindinis šio tarptautinio pobūdžio dokumento tikslas – baudžiamosios politikos suvienodinimas, siekiant apsaugoti visuomenę nuo elektroninių nusikaltimų, ir bendradarbiavimo tiriant nusikaltimus, susijusius su kompiuterinėmis sistemomis ir duomenimis, bei renkant įrodomąją informaciją, skatinimas. Dokumente pateikiama nusikalstamų veikų elektroninėje erdvėje klasifikacija, kurią perėmė ir į baudžiamuosius įstatymus įtraukė nemažai pasaulio valstybių: nusikaltimai kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui; kompiuteriniai nusikaltimai; turinio nusikaltimai ir nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais.

Lietuva Budapešto konvenciją pasirašė 2003 m. birželio 23 d., o ratifikavo 2004 m. kovo 18 d. 2021 m. kovo mėnesio duomenimis, konvenciją ratifikavo 65 valstybės, ir dar 3 yra ją pasirašiusios, tačiau neratifikavusios. Atsižvelgiant į tai, kad pasaulyje yra apie 200 valstybių, galima pritarti nuomonei[7], kad Budapešto konvencijos įtaka kovai su nusikalstamomis veikomis elektroninėje erdvėje nėra labai didelė.

Kitas paminėtinas tarptautinio pobūdžio dokumentas – Europos Tarybos 2003 m. gruodžio 13 d. priimta Europos saugumo strategija[8]. Pilnas dokumento pavadinimas yra „Saugi Europa geresniame pasaulyje“. Strategijoje išskiriamos penkios grėsmės saugumo interesams: 1) masinio naikinimo ginklų platinimas; 2) terorizmas ir organizuotas nusikalstamumas; 3) kibernetinis saugumas; 4) energetinis saugumas; 5) klimato kaita. Strategijoje pabrėžiama, kad išpuoliai prieš informacinių technologijų sistemas vertintini kaip naujas ekonominis, politinis ir karinis ginklas, todėl šioje srityje būtinas sąmoningumo ugdymas ir tarptautinio bendradarbiavimo skatinimas.

---

[4] New Zeland‘s Cyber Security Strategy, 2015. Prieiga internetu: https://dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy-december-2015.pdf

[5] Andrei Soldatov and Irina Borogan „Russia’s approach to cyber: the best defence is a good offence“. Hacks, leaks and disruptions Russian cyber strategies, Challot Papers, 2018. P. 15-24.

[6] 2001 m. Konvencija dėl elektroninių nusikaltimų. Angliškas Konvencijos tekstas: Convention on Cybercrime, prieiga internetu: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[7] W. Brenner S.W. Cybercrime: Criminal Threats from Cyberspace.// Library of Congress Cataloging, 2010, p. 209.

[8] Prieiga internetu: https://www.consilium.europa.eu/media/30821/qc7809568ltc.pdf

Europos saugumo strategiją papildo 2008 m. gruodžio 11 d. ataskaita dėl Europos saugumo strategijos įgyvendinimo „Saugumo užtikrinimas besikeičiančiame pasaulyje“[9]. Ataskaitoje pabrėžiama, kad ji nepakeičia Europos saugumo strategijos, o tik ją įtvirtina ir suteikia galimybę įvertinti pasiektus laimėjimus ir numatyti tolimesnius veiksmus jos įgyvendinimui. Kibernetinio saugumo užtikrinimo būtinybė išlieka aktuali, pabrėžiama, kad būtinas tolimesnis glaudus bendradarbiavimas šioje srityje.

Dar vienas, reikalaujantis detalesnės analizės ir itin svarbus nacionalinių kibernetinio saugumo strategijų kūrimo ir diegimo procesams dokumentas – 2013 m. Europos Sąjungos kibernetinio saugumo strategija bus aptartas 2 šio darbo skyriuje.

1.2 Nacionalinių kibernetinio saugumo strategijų kūrimo poreikio vertinimas

Europos Sąjungos tinklų ir informacijos saugumo agentūra ENISA nacionalines kibernetinio saugumo strategijas apibrėžia kaip veiksmų planus, skirtus valstybių nacionalinių infrastruktūrų saugumo ir atsparumo gerinimui. Tokio pobūdžio dokumentuose nustatomi esminiai tikslai ir prioritetai, kurie turėtų būti įgyvendinti per tam tikrą laikotarpį.

Nacionalinės kibernetinio saugumo strategijos poreikį geriausiai atskleidžia tai, kad vystantis kibernetinėms grėsmėms ir sparčiai augant jų skaičiui, kibernetinio saugumo politika tampa nacionalinės politikos prioritetu. Mokslo šaltiniuose pagrįstai teigiama, kad „nacionalinio saugumo užtikrinimas yra aukščiausias kiekvienos valstybės vidaus ir užsienio politikos tikslas“[10]. Kibernetinis saugumas priskiriamas prie kitų nacionalinių grėsmių, todėl būtinas efektyvių kovos su kibernetinio saugumo pažeidimais priemonių numatymas, parengimas ir įdiegimas. Kibernetinio saugumo stiprinimas turėtų išlikti vienu iš svarbiausių valstybės prioritetų[11]. Nacionalinė kibernetinio saugumo strategija yra pagrindinis teisės aktas valstybės mastu nustatantis tikslus, uždavinius ir prioritetines veiklos kryptis reaguojant į kibernetines grėsmes ir užtikrinant informacinių sistemų bei tinklų saugumą bei atsparumą.

2016 m. liepos 6 d. Europos Sąjungos direktyvoje 2016/1148 „Dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti“ (toliau šiame poskyryje – TIS direktyva) pateikti tam tikri reikalavimai nacionalinėms kibernetinio saugumo strategijoms, o Europos Sąjungos komisijos 2017 m. spalio 4 d. komunikato priede „Racionaliausias tinklų ir informacijos saugumas. Kaip veiksmingai įgyvendinti Direktyvą (ES) 2016/1148 dėl priemonių

[9] Prieiga internetu: https://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/LT/reports/104645.pdf
[10] A. Petrauskaitė, R. Markelienė, R. Gedminienė „Šalies saugumas ir gynyba“, Vilnius 2016 m. P. 9.
[11] P. Saudargas “Kibernetinių atakų Lietuvoje atvejai ir kaip į juos reaguojama“. Kibernetinio saugumo apžvalga, 2016 m. P. 29.

aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti" tie reikalavimai detalizuoti. Vis dėlto, kibernetinio saugumo strategijos rengimas, diegimas ir įgyvendinimas yra sudėtingas ir daug laiko atimantis procesas. Dėl šios priežasties ENISA parengė Kibernetinio saugumo strategijų rengimo ir diegimo rekomendacijas[12]. ENISA parengtame Kibernetinio saugumo strategijų rengimo ir tobulinimo vadove numatyti šie pagrindiniai nacionalinės kibernetinio saugumo strategijos rengimo etapai:

1) nustatyti viziją, apimtį, tikslus ir prioritetus;

2) laikytis rizikos vertinimo metodo;

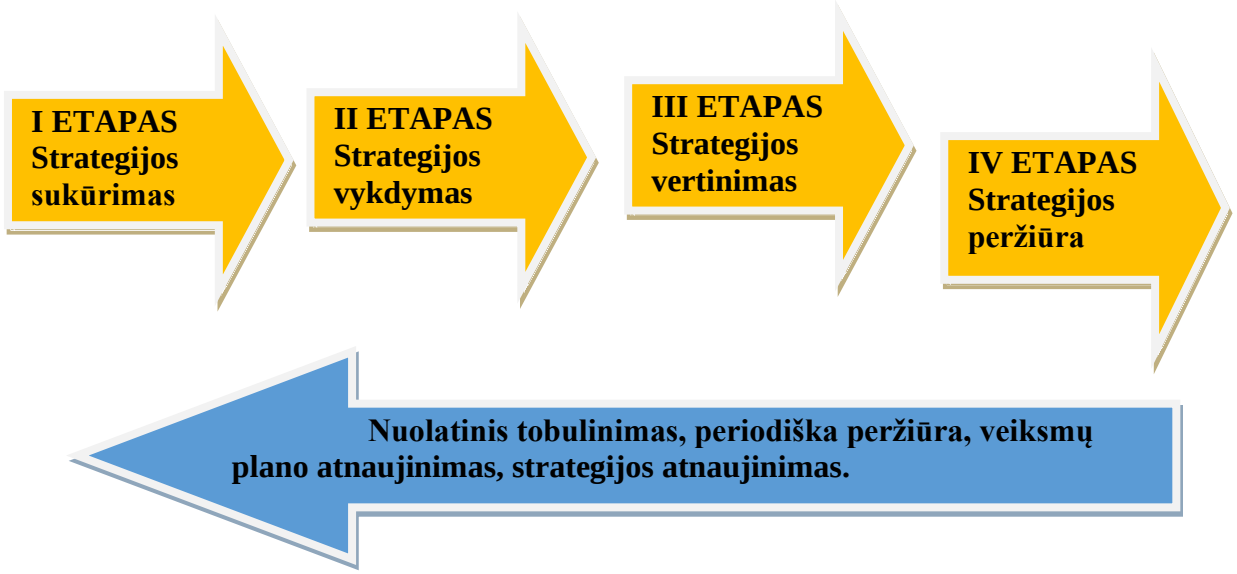
3) apžvelgti galiojančią politiką, taisykles ir galimybes;

4) nustatyti aiškią valdymo struktūrą;

5) nustatyti ir įtraukti suinteresuotus subjektus;

6) sukurti patikimus keitimosi informacija mechanizmus.

Svarbu pažymėti ir tai, kad kibernetinio saugumo strategijos kūrimo ir įgyvendinimo procesas – tęstinis, t. y. sukuriama strategija, siekiama joje nustatytų tikslų ir uždavinių įgyvendinimo pagal parengtą veiksmų planą, strategijos įgyvendinimas periodiškai įvertinamas tiek pasiektų tikslų ir įgyvendintų uždavinių, tiek jų aktualumo atžvilgiu, atliekamas strategijos keitimas, atnaujinimas.



2 Pav. Strategijos kūrimo ir įgyvendinimo procesas

Šaltinis: NCSS Good Practice Guide, 2016, p. 13.

Minėti kibernetinio saugumo strategijos rengimo etapai bei TIS direktyvoje nurodyti esminiai klausimai, kurie turėtų būti aptarti kiekvienos šalies kibernetinio saugumo strategijoje, leidžia kritiškai

[12] ENISA, National Cyber Security Strategies: *An Implementation Guide, 2012.* Prieiga per internetą: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide; ENISA, *NCSS Good Practice Guide, 2016.* Prieiga per internetą: https://www.enisa.europa.eu/publications/ncss-good-practice-guide; ENISA, *An evaluation framework for Cyber Security Strategies, 2014.* Prieiga internetu: https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies

įvertinti parengtos ir įdiegtos strategijos privalumus ir trūkumus, todėl jais bus vadovaujamasi analizuojant pasirinktų valstybių kibernetinio saugumo strategijas, nepriklausomai nuo to, patenka tos valstybės į TIS direktyvos reguliavimo sritį, ar ne. Analizuojant atskirų valstybių kibernetinio saugumo strategijas bus atsižvelgta į šiuos aspektus: strategijos apimtį, naujumą, išdėstymo struktūrą; strategijoje numatytus tikslus, principus, uždavinius; šio dokumento sąsajas su kitais dokumentais; numatytas grėsmes, strategijos įgyvendinimo veiksmų planą (jei toks yra); subjektus, dalyvaujančius strategijos įgyvendinime ir kiekvienos analizuojamos kibernetinio saugumo strategijos ypatumus bei į gerosios praktikos pavyzdžius, kurie būtų naudingi ir galėtų būti pritaikyti Lietuvos nacionalinėje kibernetinio saugumo strategijoje.

1.3 Europos Sąjungos kibernetinio saugumo agentūros 2016 m. tyrimo ir BSA Programinės įrangos aljanso 2015 m. tyrimo dėl nacionalinių kibernetinio saugumo strategijų apžvalga

Prieš pradedant nagrinėti pasaulio valstybių kibernetinio saugumo strategijų ypatumus, įdomu paanalizuoti, kokius nacionalinių kibernetinio saugumo strategijų trūkumus įžvelgė Europos Sąjungos kibernetinio saugumo agentūra (toliau šiame poskyryje – ENISA) 2016 m. lapkričio 14 d. publikuotame valstybių nacionalinių kibernetinio saugumo strategijų turinio ir jų įgyvendinimo tyrime ir BSA Programinės įrangos aljanso[13] 2015 m. publikuotame Europos Sąjungos kibernetinio saugumo būklės tyrime.

ENISA 2016 m. tyrime[14] analizuoti šie esminiai nacionalinių kibernetinio saugumo strategijų turinio ir įgyvendinimo aspektai: vizijos, taikymo srities, tikslų ir prioritetų nustatymas; rizikų vertinimo metodologijos įdiegimas; teisinio reglamentavimo peržiūra ir tobulinimas; aiškios valdymo struktūros sukūrimas ir įdiegimas; visų suinteresuotųjų šalių įtraukimas; patikimų keitimosi informacija mechanizmų įdiegimas. Tyrimo metu analizuotos 22 valstybių kibernetinio saugumo strategijos. Iš šiame darbe analizuotų strategijų ENISA tyrime aptartos Prancūzijos ir Ispanijos strategijos.

Trumpai aptarsiu tyrimo rezultatus pagal minėtus esmines tyrimo sritis.

1. *Vizijos, taikymo srities, tikslų ir prioritetų nustatymas*. Pastebėta, kad strategijose formuluojami panašūs tikslai ir jose numatytos taikymo sritys (kritinės informacijos infrastruktūros objektų apsauga, bendradarbiavimas su privačiu sektoriumi, teisėkūros tobulinimas, atsakingų už kibernetinio saugumo priemonių vykdymą institucijų steigimas) iš esmės nesiskiria.

[13] BSA (The Software Alliance), vadinama „BSA | The Software Alliance“, yra „Microsoft“ įkurta prekybos grupė, kuri bando panaikinti jos narių sukurtos programinės įrangos piratavimą

[14] Prieiga internetu: https://www.enisa.europa.eu/publications/ncss-good-practise-guide

2. *Rizikų vertinimo metodologijos įdiegimas*. Idealiu atveju metodologija turėtų apimti rizikos nustatymą, jos analizę ir vertinimą (stebėseną ir kontrolę). Skatintinas rizikos vertinimas tiek nacionaliniu, tiek atskirų sektorių lygmenimis ir pastebima, kad valstybės, vertindamos riziką nacionaliniu lygmeniu, stengiasi įtraukti visas įmanomas grėsmes – nuo elektroninių nusikaltimų iki tam tikrų techninių nesklandumų. Ispanijos kibernetinio saugumo strategija pateikiama kaip gerosios praktikos pavyzdys, nes joje rizikos vertinimas vykdomas strateginiu-politiniu, operaciniu ir taktiniu-techniniu lygmenimis.

3. *Teisinio reglamentavimo peržiūra ir tobulinimas*. Šioje srityje valstybės su rimtesnėmis problemomis nesusiduria. Atkreipiamas dėmesys į tai, kad didžioji dalis į tyrimo sritį patekusių valstybių spėjo priimti antrąsias kibernetinio saugumo strategijas, kurios, palyginus su pirmosiomis, konkretesnės, turinčios kibernetinio saugumo priemonių įgyvendinimo planus, ko pasigendama pirmosiose strategijose.

4. *Aiškios valdymo struktūros sukūrimas ir įdiegimas*. Pastebėta, kad pirmosiose valstybių kibernetinio saugumo strategijose buvo numatyta įkurti atsakingas institucijas, tokias kaip Nacionaliniai kibernetinio saugumo centrai, antrosiose – plečiamos ir detalizuojamos jau įkurtų institucijų funkcijos. Tyrimo metu nustatyta, kad valstybės renkasi tiek centralizuotą (pagrindinė kibernetinio saugumo institucija koordinuoja kitų į valdymo struktūrą įtrauktų subjektų veiksmus)[15], tiek decentralizuotą[16] (atsakingos institucijos vadovaujasi bendradarbiavimo ir subsidiarumo principais) valdymo struktūrą.

5. *Visų suinteresuotųjų subjektų įtraukimas*. Pastebėta, kad bendradarbiavimas su privačiu sektoriumi analizuotose valstybėse skiriasi. Vienose valstybėse bendradarbiavimas vyksta partnerystės pagrindu, kitos apsiriboja tam tikrų įgaliojimų ir įpareigojimų privataus sektoriaus subjektams suteikimu nacionaliniuose teisės aktuose. Kaip gerosios praktikos pavyzdžiai nurodomos Estijos ir Austrijos kibernetinio saugumo strategijos, kuriose numatyta, kad privataus sektoriaus subjektai įtraukiami į esminių sprendimų kibernetinio saugumo srityje priėmimo procesą (Austrija) ar dalyvauja darbo grupėse, sprendžiančiose šiuos klausimus (Estija).

6. *Patikimų keitimosi informacija mechanizmų įdiegimas.* Šioje srityje Olandijos įdiegta keitimosi informacija sistema pateikiama kaip sektinas pavyzdys. Šalyje veikia Nacionalinis reagavimo tinklas, skirtas viešojo ir privataus sektorių keitimuisi informacija, taip pat dalijimuisi žiniomis ir patirtimi, bei Nacionalinis aptikimo tinklas – informacinė platforma, kurioje keičiamasi informacija apie grėsmes ir skaitmeninius pavojus.

[15] Centralizuoto valdymo pavyzdžiu galėtų būti Prancūzija, kurioje koordinavimo funkcijos suteiktos 2009 m. įsteigtai Tinklų ir informacijos apsaugos agentūrai.

[16] Švedijoje atsakomybė už kibernetinio saugumo priemonių įgyvendinimo koordinavimą suteikta savivaldybėms ir įvairioms viešosioms institucijoms.

Taip pat norėčiau paminėti, kad ENISA nustatė sritis, kuriose valstybėms sunkiausiai sekėsi įgyvendinti strategijose numatytas kibernetinio saugumo priemones: privataus sektoriaus investicijų į kibernetinio saugumo užtikrinimą pritraukimas (sėkme gali džiaugtis tik 3 tirtos valstybės), bendradarbiavimas su privačiu sektoriumi (tai pavyko tik 8 tirtoms valstybėms), balanso tarp privatumo ir saugumo išlaikymas (įgyvendino 9 valstybės).

Visoms tirtoms valstybėms pavyko įdiegti reagavimo į kibernetinius incidentus sistemą ir įsitraukti į tarptautinį bendradarbiavimą, taip pat dauguma tirtų valstybių (18) organizavo kibernetinio saugumo pratybas.

BSA 2015 m. tyrimas[17] apėmė 28 valstybių kibernetinio saugumo strategijas. Strategijos buvo analizuojamos pagal šiuos esminius kriterijus: *teisinę bazę* (ar valstybė turi patvirtintą kibernetinio saugumo strategiją, kibernetinio saugumo priemonių įgyvendinimo planą, ar teisiškai reglamentuota kibernetinio saugumo būklės stebėsena, kritinės svarbos infrastruktūros apsauga, bendradarbiavimas su privačiu sektoriumi), *atsakingų subjektų paskyrimą* (ar įsteigtas nacionalinis kibernetinio saugumo centras, ar sukurta platforma informavimui apie kibernetinius incidentus, ar įsteigtas reagavimo į kibernetinius incidentus padalinys), *partnerystę su privačiu sektoriumi* (yra, ar nėra, kaip organizuojama), *kibernetinio saugumo priemonių planų kūrimą pagal atskirus sektorius* ir *švietimą* (ar numatytos specialios švietimo programos, jaunimo supažindinimas su kibernetinėmis grėsmėmis).

Tyrimo rezultatai pateikti lentelėse, kuriose pagal kiekvienam iš nurodytų kriterijų suformuluotus klausimynus valstybė vertinama kaip įvykdžiusi atitinkamą priemonę, įvykdžiusi iš dalies, neįvykdžiusi. Taip pat pateikiamas trumpas kiekvienos analizuotos valstybės pasiekimų įgyvendinant numatytas kibernetinio saugumo priemones apibendrinimas.

Tyrimo metu Lietuvoje galiojo Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa[18], todėl BSA tyrime buvo vertinamos šio dokumento nuostatos ir jame numatytos kibernetinio saugumo priemonės. Prasčiausiai Lietuvai sekėsi įgyvendinti kibernetinio saugumo priemonių planų kūrimo pagal atskirus sektorius kriterijų, visi šios dalies klausimyno elementai vertintini kaip neįvykdyti. Taip pat Lietuva sulaukė kritikos dėl tik formalaus bendradarbiavimo su privačiu sektoriumi įtvirtinimo ir informacijos apie numatytų kibernetinio saugumo priemonių įgyvendinimą trūkumo ar riboto prieinamumo.

[17] Prieiga internetu: http://cybersecurity.bsa.org/index.html

[18] Patvirtinta Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796. Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.403385

2. KIBERNETINIO SAUGUMO STRATEGIJŲ KŪRIMO IR DIEGIMO PASAULINĖ PATIRTIS

2.1 Strateginiai prioritetai 2013 m. Europos Sąjungos kibernetinio saugumo strategijoje

2013 m. Europos Sąjungos kibernetinio saugumo strategija „Atvira, saugi ir patikima kibernetinė erdvė“[19] (toliau šiame poskyryje – Kibernetinio saugumo strategija) priimta Briuselyje 2013 m. vasario 7 d. Dokumento įžangoje pabrėžiama, kad kibernetinė erdvė daro didžiulį poveikį visoms gyvenimo sritims, todėl tiek mūsų pagrindinės teisės ir laisvės, tiek socialinė sąveika ir ekonomika priklauso nuo sklandaus informacinių technologijų veikimo. Strategijoje išdėstoma Europos Sąjungos vizija kibernetinio saugumo srityje, išvardijami veiksmai, kurių būtina imtis, kad Europos Sąjungos internetinė aplinka taptų saugiausia pasaulyje. Aptarsiu Kibernetinio saugumo strategijoje numatytus saugumo principus ir strateginius prioritetus.

Kibernetinio saugumo strategijoje išskiriami šie penki principai:

1) *Europos Sąjungos pagrindinės vertybės galioja ir skaitmeniniame, ir fiziniame pasaulyje* (kibernetinėje erdvėje taikomi teisės aktai nesiskiria nuo teisės aktų, taikomų kitose gyvenimo srityse).

2) *Pagrindinių teisių, žodžio laisvės, asmens duomenų ir privatumo apsauga* (pagrindinės teisės traktuojamos kaip kibernetinio saugumo veiksmingumo pagrindas ir atvirkščiai, be saugių informacinių technologijų ir sistemų pagrindinių teisių užtikrinti neįmanoma. Pabrėžiama, kad dalijimasis bet kokio pobūdžio informacija, susijusia su asmens duomenimis, turi būti vykdomas nepažeidžiant individo teisių).

3) *Prieiga visiems* (principo esmė ta, kad kiekvienas individas turi turėti galimybę naudotis internetu ir gauti jam reikiamą informaciją, todėl turi būti užtikrintas interneto vientisumas ir saugumas). Kiek šį principą įmanoma realiai įgyvendinti – ginčytinas klausimas. Plačiau tai aptarsiu analizuodama Europos Komisijos 2017 m. atliktą Kibernetinio saugumo strategijos įvertinimą.

4) *Demokratiškas ir veiksmingas daugelio suinteresuotųjų šalių dalyvavimu grindžiamas valdymas* (principo esmė ta, kad skaitmeninio pasaulio nekontroliuoja kuris nors vienas subjektas; svarbus visų suinteresuotųjų šalių įsitraukimas ir dalyvavimas).

5) *Bendra atsakomybė siekiant užtikrinti saugumą* (atsiradusį pažeidžiamumą reikia tinkamai apibrėžti, išnagrinėti, pašalinti arba sumažinti. Atsakomybė (valdžios institucijų, privataus sektoriaus ar atskirų individų) bendra, reaguojama koordinuotai).

[19] Prieiga internetu: https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX:52013JC0001

Valstybės, rengdamos nacionalines kibernetinio saugumo strategijas, į jas įtraukia savo turiniu tapačius ar panašius principus, tokius kaip proporcingumas, bendradarbiavimas, atsakomybė, esminių teisių ir laisvių apsauga, rizikų valdymas. Vieningos principų pateikimo sistemos nėra.

Kibernetinio saugumo strategijoje numatyti **strateginiai prioritetai ir veiksmai:**

1. Kibernetinio atsparumo pasiekimas. Puikiai suvokiant, kad visiškas kibernetinio atsparumo pasiekimas sunkiai įsivaizduojamas, tikslas vertintinas kaip itin ambicingas, nors priemonės, numatytos jo įgyvendinimui pasiekti, pakankamai realios. Numatoma teisės aktu nustatyti mažiausius bendrus nacionalinio lygmens tinklų ir informacijos saugumo reikalavimus (kompetentingos institucijos paskyrimas, nacionalinės strategijos ir nacionalinio bendradarbiavimo plano parengimas), parengti koordinuotos prevencijos, aptikimo, pasekmių švelninimo ir reagavimo mechanizmus, leidžiančius kompetentingoms nacionalinėms institucijoms bendradarbiauti, keistis informacija, taip pat skatinti ir stiprinti privataus sektoriaus įsitraukimą.

2. Radikalus elektroninių nusikaltimų skaičiaus sumažinimas. Pabrėžiama, kad šio tikslo įgyvendinimas neįmanomas be griežtų ir veiksmingų teisės aktų priėmimo, atskirų padalinių, kurių paskirtis būtų kova su nusikalstamumu elektroninėje erdvėje, steigimo, bendradarbiavimo su Europolo struktūroje sukurtu Europos kovos su elektroniniu nusikalstamumu centru ir Europos Sąjungos lygmens koordinavimo gerinimu.

3. Kibernetinės gynybos politikos ir pajėgumų, susijusių su bendra saugumo ir gynybos politikos sistema, plėtojimas. Pažymima, kad atsižvelgiant į grėsmių įvairovę būtina stiprinti modelių, kuriuos taiko civiliai ir kariškiai, saugodami ypač svarbius kibernetinius išteklius, sinergiją. Skatinamas kibernetinės gynybos pajėgumų plėtojimas aptikimo, reagavimo ir atkūrimo po sudėtingų kibernetinių grėsmių segmentuose.

4. Pramonės ir technologinių išteklių plėtra siekiant kibernetinio saugumo. Šio tikslo įgyvendinimui numatoma nemažai priemonių, kurių didelė dalis susijusi su technologinių inovacijų diegimu, t. y. skatinama kurti bendrąją kibernetinio saugumo prekių rinką, kurioje aukštą kibernetinio saugumo lygį užtikrinančios prekės galėtų turėti išskirtinį ženklinimą ir taip įgytų konkurencinį pranašumą. Taip pat numatoma remti saugumo standartų plėtrą, pagalba savanoriškų sertifikavimo schemų nuotolinės kompiuterijos srityje plėtrai. Skatinamos investicijos moksliniams tyrimams, technologijų plėtrai, inovacijų skatinimui.

5. Nuoseklios Europos Sąjungos kibernetinės politikos sukūrimas ir Europos Sąjungos pagrindinių vertybių rėmimas. Šiuo aspektu kibernetinės erdvės klausimai siejami su Europos Sąjungos išorės santykiais ir bendra išorės ir saugumo politika.

Pažymėtina, kad Kibernetinio saugumo strategija vertintina kaip išsami Europos Sąjungos vizija, kaip geriausiai užkirsti kelią kibernetinės veiklos sutrikdymui bei atakomis ir kokių atsakomųjų

priemonių imtis[20]. Nepaisant to, įgyvendinant šiame dokumente numatytus strateginius prioritetus, susidurta su nemažai iššūkių, todėl rezultatai, vadovaujantis Europos Komisijos 2017 m. atliktu Kibernetinio saugumo strategijos įvertinimu[21], kuklūs.

Nurodytame įvertinime pažymima, kad Kibernetinio saugumo strategijoje numatyti prioritetai neprarado aktualumo, tačiau naujos grėsmės neišsprendžiamos, numatyti tikslai pasiekti tik iš dalies, ką lėmė pakankamai abstraktus prioritetų suformulavimas ir neatsižvelgimas į tam tikrus svarbius aspektus.

Prioritetas *pasiekti kibernetinį atsparumą* neįgyvendintas ne tik dėl to, kad visiško kibernetinio atsparumo pasiekimas neįmanomas, dėl ko šis prioritetas traktuotinas kaip vizija, bet ir dėl to, kad numatyti bendradarbiavimo mechanizmai buvo riboti, valstybių narių bendradarbiavimas grindžiamas savanoriškumo principu, o privataus sektoriaus įsitraukimas vis dar yra ankstyvojoje stadijoje. Prioritetas *radikaliai sumažinti elektroninių nusikaltimų skaičių* taip pat neįgyvendintas. Tai įtakojo tiek augantis nusikalstamų veikų elektroninėje erdvėje skaičius, tiek jų nustatymo ir tyrimo sunkumai, Ženklesnių rezultatų imantis priemonių prieš seksualinio vaikų išnaudojimo internete atvejus taip pat nepasiekta – tokio pobūdžio nusikalstamų veikų skaičius nesumažėjo. Pastabėta, kad šis prioritetas suformuluotas pernelyg ambicingai, jo esmė galėjo būti sukoncentruota į tikslą – kovoti su elektroniniais nusikaltimais, siekiant užtikrinti geresnę visų vartotojų apsaugą.

Pastebėta, kad prioritetas *plėtoti pramonės ir technologinius išteklius* įgyvendinamas lėtai ir fragmentiškai, rezultatai kuklūs. Valstybių narių pastangos dalyvauti Europos Sąjungos kibernetinės erdvės gynyboje dar labai menkos, trūksta efektyvių mechanizmų ir valstybių narių koordinuotų veiksmų kuriant kibernetinį atsparumą trečiosiose valstybėse, tačiau padaryta pažanga *kuriant nuoseklią tarptautinę kibernetinio saugumo politiką.*

2020 m. gruodžio 16 d. Europos Komisija pristatė naują Europos Sąjungos kibernetinio saugumo strategiją[22]. Strategijos tikslas – padidinti Europos atsparumą kibernetinėms grėsmėms ir užtikrinti, kad tiek fiziniai, tiek juridiniai subjektai galėtų visapusiškai ir saugiai naudotis skaitmeninėmis priemonėmis. Strategijoje pateikiami konkretūs pasiūlymai dėl reguliavimo, investicijų ir politikos šiose srityse:

1. Atsparumas, technologinis suverenumas ir lyderystė. Siūloma pertvarkyti tinklų ir informacinių sistemų saugumo taisykles, taip didinant viešojo ir privataus sektorių ypatingos svarbos subjektų, tokių kaip ligoninės, elektros energijos tinklai, geležinkeliai, kitų ypatingos svarbos infrastruktūros subjektų ir paslaugų kibernetinį saugumą. Taip pat rekomenduojama sukurti visoje

[20] Darius Štitilis „Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos“. Socialinės technologijos, 2013, 3(1). P. 192.
[21] Prieiga internetu: http://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0- 0.PDF
[22] Prieiga internetu: The Cybersecurity Strategy | Shaping Europe's digital future (europa.eu)

Europos Sąjungos teritorijoje veikiantį dirbtiniu intelektu grindžiamą saugumo operacijų centrų tinklą, gebantį aptikti kibernetinio išpuolio požymius ir imtis aktyvių kelio jam užkirtimo ar neutralizavimo veiksmų dar prieš patiriant žalą.

2. Prevencijos, atgrasymo ir reagavimo operatyvinių pajėgumų stiprinimas. Įgyvendinant šį pasiūlymą ketinama ir toliau skatinti bendradarbiavimą kibernetinės gynybos srityje, sukuriant naują bendrą kibernetinio saugumo padalinį, bei plėtoti pažangiausius kibernetinės gynybos pajėgumus.

3. Spartesnis atsparios pasaulinės kibernetinės erdvės kūrimas aktyvesnio bendradarbiavimo dėka. Strategijoje pabrėžiama, kad ketinama vykdyti aktyvesnį bendradarbiavimą su šalimis narėmis, siekiant stiprinti saugumą ir stabilumą kibernetinėje erdvėje, taip pat ginti žmogaus teises ir pagrindines laisves internete.

Europos Sąjungos taryba, 2021 m. kovo 22 d. pranešime spaudai[23] pristatė išvadas dėl naujosios Europos Sąjungos kibernetinio saugumo strategijos, kuriose pabrėžė, kad kibernetinis saugumas itin svarbus, norint sukurti „atsparią, žalią ir skaitmeninę Europą“, akcentavo būtinybę stiprinti gebėjimą savarankiškai priimti sprendimus kibernetinio saugumo srityje, stiprinant skaitmeninę lyderystę ir strateginius pajėgumus.

2.2 2016 m. liepos 6 d. Europos Sąjungos direktyvos 2016/1148 „Dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti“ reikšmė nacionalinių kibernetinio saugumo strategijų kūrimui

Europos Sąjungos valstybių narių pasirengimas užtikrinti aukštą tinklų ir informacinių sistemų saugumo lygį niekuomet nebuvo vienodas. Tai lėmė nevienodą vartotojų ir įmonių apsaugos lygį, taip pat kenkė bendram tinklų ir informacinių sistemų saugumo lygiui Sąjungoje. Be to, nesant bendrų reikalavimų esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams, nebuvo įmanoma sukurti veiksmingo bendradarbiavimo mechanizmo Sąjungos lygmeniu. Šios priežastys ir paskatino sukurti dokumentą, numatantį priemones, padėsiančias pasiekti aukštą tinklų ir informacinių sistemų saugumo lygį Europos Sąjungoje.

2016 m. liepos 6 d. Europos Sąjungos direktyva 2016/1148 „Dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti“ (toliau – TIS direktyva), numatanti priemones tinklų ir informacinių sistemų saugumui užtikrinti ir nustatanti pareigą visoms valstybėms narėms priimti nacionalines tinklų ir informacinių sistemų saugumo strategijas, vertinama prieštaringai. TIS direktyvos rengimo procesas nebuvo lengvas ir paprastas. 2013 m. vasario 7 d.

[23] Plačiau: https://www.consilium.europa.eu/lt/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/

svarstymui pateiktame direktyvos projekte[24], kuriuo siūloma numatyti priemones užtikrinti aukštą bendrą tinklų ir informacijos saugumo lygį, dar 2014 m. buvo atlikta nemažai pakeitimų, tokių kaip aiškesnių parametrų kibernetiniams incidentams, apie kuriuos būtina pranešti, nustatymas, kritinės infrastruktūros sąrašo išplėtimas, galimybės valstybėms paskirti daugiau nei vieną instituciją, atsakingą už kibernetinį saugumą, numatymas ir kitų. Vėliau pateikti šie projekto tikslinimai ir pastabos: rizikų valdymo praktikas bei pareigą pranešti apie saugumo pažeidimus taikyti visai rinkai bei debesijos paslaugų teikėjus išlaikyti direktyvos veikimo srityje.

Priimtoje TIS direktyvoje numatyti aiškūs įpareigojimai valstybėms narėms, kurie privalėjo būti įgyvendinti iki 2018 m. gegužės 9 d. Pažymėtina, kad Lietuvos Respublikos kibernetinio saugumo įstatymas[25] (2018 m. liepos 4 d. redakcija) suderintas su TIS direktyvos nuostatomis.

Lietuvos ekspertų nuomonės dėl TIS direktyvos veiksmingumo ir pagrįstumo išsiskiria. Teigiama[26] (šiai nuomonei pritaria ir autorius), kad šią direktyvą galima laikyti vienu geriausių tarpvalstybinio bendradarbiavimo pavyzdžių. Ji sukuria sistemą ir numato procedūras, kaip užtikrinti bendradarbiavimą ir bendrą koordinavimą tarp kibernetiniu saugumu besirūpinančių Europos Sąjungos valstybių narių. Tai neabejotinai vienas svarbiausių žingsnių skatinant tarptautinį bendradarbiavimą. Direktyva įpareigoja nacionalines už kibernetinį saugumą atsakingas institucijas perduoti informaciją apie kibernetinius incidentus Europos Sąjungos ryšių ir informacijos saugumo agentūrai (toliau – ENISA), kuri sudaro galimybes apie incidentus informuoti visas Europos Sąjungos valstybes nares.

Yra ir kardinaliai skirtingų nuomonių: į direktyvos veikimo lauką įtraukus tokias skaitmenines paslaugas kaip elektroninės parduotuvės, paieškos sistemos ar duomenų talpyklos, baiminamasi dėl vartotojų privatumo užtikrinimo. TIS direktyva sulaukia nemažai kritikos ir dėl nepakankamo jos nuostatų vykdymo reglamentavimo, galinčio lemti skirtingą direktyvos vykdymą atskirose valstybėse[27].

Europos Sąjungos komisijos 2017 m. spalio 4 d. komunikate Europos Parlamentui ir Tarybai nurodoma, kad TIS direktyva yra pirmasis kibernetinio saugumo iššūkiams skirtas Europos Sąjungos horizantalusis teisės aktas. Direktyva, kurios esminis tikslas – pasiekti bendrą aukštą tinklų ir informacinių sistemų saugumo lygį Europos Sąjungoje, suteikia pagrindą reaguoti į didėjančias kibernetines grėsmes ir iššūkius. Be to, kas itin svarbu šiam darbui, TIS direktyva skatina valstybes nares peržiūrėti savo nacionalines kibernetinio saugumo strategijas, šalinti jų spragas ir pasinaudoti

[24] Prieiga internetu: EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive | Shaping Europe's digital future (europa.eu)
[25] Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr
[26] Justinas Kulys „Trumpa įžanga į kibernetinį saugumą". Apžvalga, 2019-05-02. Prieiga internetu: http://apzvalga.eu/trumpa-izanga-i-kibernetini-sauguma.html
[27] Albert Komar „Tinklų ir informacinių sistemų saugumo direktyva – didžiulės ambicijos ir neapibrėžtos priemonės". Kibernetinio saugumo apžvalga, 2016 m. P. 29-31.

gerąja praktika tobulinant šiuos dokumentus[28]. Pažymėtina, kad nacionalinėmis kibernetinio saugumo strategijomis turėtų būti siekiama daugiau, negu minimaliai reikalaujama TIS direktyvoje, t. y. jos turėtų būti taikomis ne vien TIS direktyvos II priede išvardytiems sektoriams (energetika, transportas, bankininkystė, finansų rinkų infrastruktūros objektai, sveikatos priežiūros sektorius, geriamo vandens tiekimas ir paskirstymas, skaitmeninė infrastruktūra) ir III priede nurodytoms paslaugoms (elektroninės prekyvietės, interneto paieškos sistemos ir debesijos kompiuterijos paslaugos). Be to, nereikėtų pamiršti ir adekvačių finansinių ir žmogiškųjų išteklių reikšmės, nes be jų apie veiksmingą nacionalinių kibernetinio saugumo strategijų įgyvendinimą neverta net užsiminti.

Būtina trumpai aptarti TIS direktyvos 7 straipsnyje numatytus reikalavimus nacionalinėms kibernetinio saugumo strategijoms. Nacionalinėje kibernetinio saugumo strategijoje privaloma:

1. Remiantis naujausia rizikos ir incidentų analize, nustatyti strategijos tikslus ir prioritetus. Tikslai turėtų būti konkretūs, išmatuojami, pasiekiami, realūs ir įvykdytini per nustatytą laiką. Strategijoje turi būti nurodytos įgyvendinimo priemonės, veiksmai, kuriuos reikia atlikti per tam tikrą laiką, taip pat pagrindiniai veiklos rezultatų rodikliai, pagal kuriuos, praėjus nustatytam įgyvendinimo laikotarpiui, ją reikia vertinti, tobulinti ir gerinti;

2. Sukurti strategijos tikslų ir prioritetų įgyvendinimui skirtą valdymo sistemą. Akcentuojama atskaitomybė politiniu lygmeniu, o sprendimų priėmimo ir išteklių skirstymo procese privaloma atsižvelgti tiek į kibernetinio saugumo ekspertų, tiek į suinteresuotųjų pramonės subjektų nuomones;

3. Nustatyti parengties, reagavimo ir atkūrimo priemones, įskaitant viešojo ir privataus sektorių bendradarbiavimą;

4. Nurodyti švietimo, informuotumo didinimo ir mokymo programas, taip pat mokslinių tyrimų ir plėtros planus.

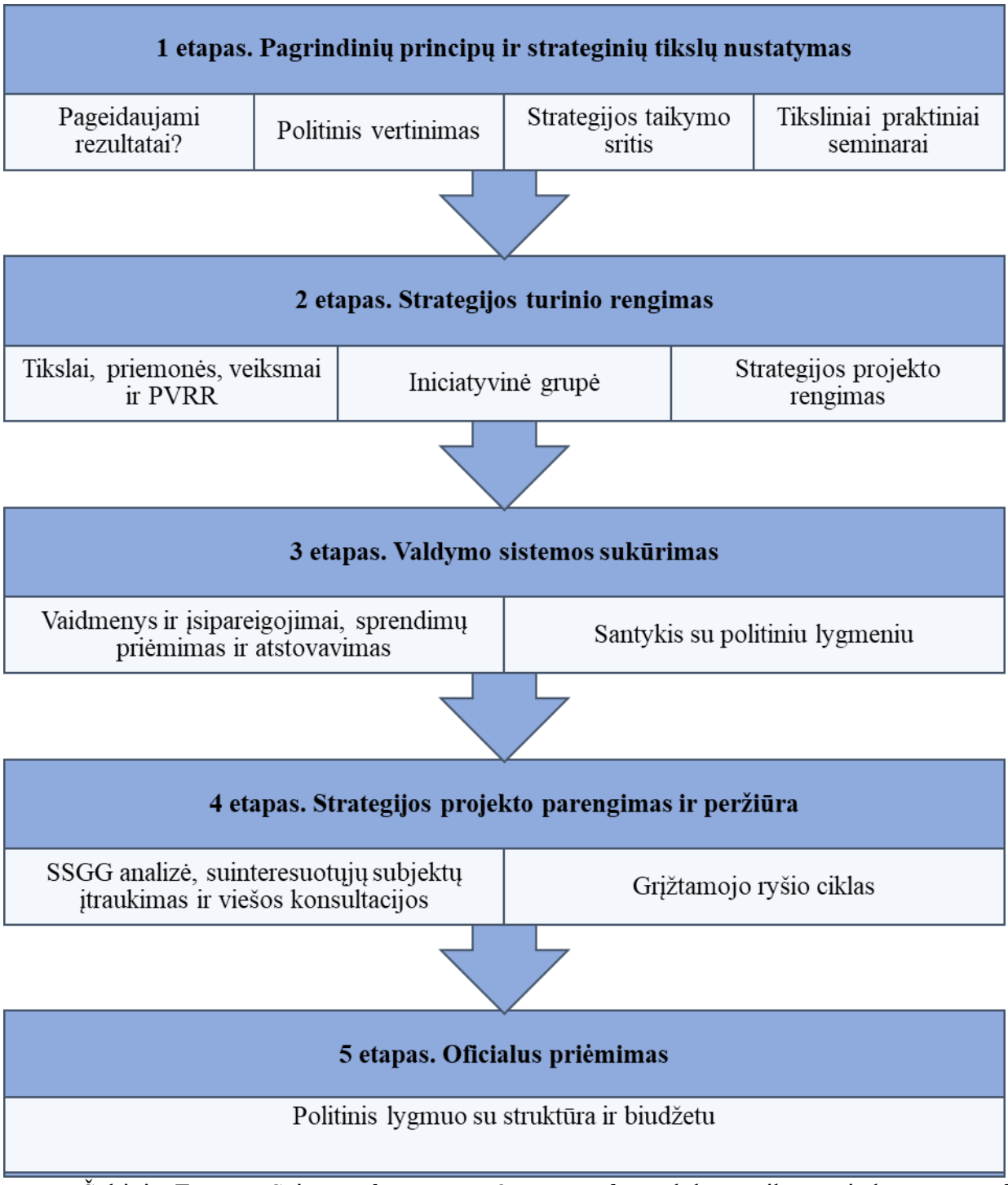
Kartu su nacionaline kibernetinio saugumo strategija turi būti parengtas ir bendradarbiavimo planas, atitinkantis bent jau šiuos reikalavimus: 1) parengtas rizikos įvertinimo planas, skirtas rizikai nustatyti ir galimų kibernetinių incidentų poveikiui įvertinti; 2) nustatyta plano įgyvendinime dalyvaujančių subjektų funkcijos ir atsakomybė; 3) numatyti bendradarbiavimo procesai, užtikrinantys kibernetinių incidentų prevenciją, nustatymą, atsakomuosius veiksmus, atstatymo bei atkūrimo procesus; 4) įtraukiamos pratybų ir mokymų gairės, įgyta patirtis registruojama ir taip pat įtraukiama į atnaujintą planą.

Europos Sąjungos komisijos 2017 m. spalio 4 d. komunikato priede „ Racionaliausias tinklų ir informacijos saugumas. Kaip veiksmingai įgyvendinti Direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti”

[28] Europos Sąjungos komisijos 2017 m. spalio 4 d. komunikato 4 p. Plačiau: https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52017DC0476&from=en

pateikiama aiški penkių etapų nacionalinių kibernetinio saugumo strategijų priėmimo procesą iliustruojanti schema:

3 Pav. Penkių etapų NKSS priėmimo procesas



Šaltinis: Europos Sąjungos komisijos 2017 m. spalio 4 d. komunikato priedo „ Racionaliausias tinklų ir informacijos saugumas. Kaip veiksmingai įgyvendinti Direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti” 9 p.

Tai, kaip valstybėms sekasi kurti ir diegti nacionalines kibernetinio saugumo strategijas ir ar jos atitinka aukščiau nurodytus reikalavimus, bus aptarta kituose šio skyriaus poskyriuose, analizuojant pasirinktų pasaulio valstybių kibernetinio saugumo strategijas.

2.3 Pirmosios nacionalinės kibernetinio saugumo strategijos, jų turinio esminiai aspektai

Prieš pradedant analizuoti pirmųjų nacionalinio kibernetinio saugumo strategijų turinį, būtina pažymėti, kad „pirmosios“ šio poskyrio kontekste reiškia nacionalinio kibernetinio saugumo strategijas, kurias valstybės priėmė ir įdiegė iki Europos Sąjungos kibernetinio saugumo strategijos priėmimo (2013 m. vasario 7 d.). Tokių valstybių Europos Sąjungoje buvo 13, taip pat nacionalines kibernetinio saugumo strategijas buvo priėmusios Jungtinė Karalystė, Jungtinės Amerikos Valstijos, Japonija, Kanada, Australija.

Detaliau bus aptartos Jungtinių Amerikos Valstijų (2011 m.), Japonijos (2010 m.), Suomijos (2010 m.) ir Australijos (2009 m.) kibernetinio saugumo strategijos.

Jungtinių Amerikos Valstijų 2011 m. kibernetinio saugumo strategija[29] išsiskiria tuo, ko trūksta daugeliui kitų valstybių strategijų – privataus sektoriaus įtraukimu. Įtraukimas jokiu būdu nėra tik deklaratyvus, privataus sektoriaus subjektams priskiriamos aiškios funkcijos ir atsakomybė už jų neįgyvendinimą. Privataus sektoriaus subjektai prisiima visišką atsakomybę už jų naudojamų technologijų ir tinklų saugumą, tačiau jokie esminiai su tuo susiję teisinio reglamentavimo aspektai nepriimami be privataus sektoriaus dalyvavimo. Pabrėžiama, kad informacijos ir tinklų saugumas – bendra atsakomybė, todėl su tuo susijusios problemos sprendžiamos bendrai, įtraukiant visus suinteresuotus subjektus. Kiti svarbūs ir sektini aspektai – parama mokslui, inovacijoms, taip pat sistemos, leidžiančios tiek aukščiausiu (valstybiniu), tiek atskirų valstijų, tiek privataus sektoriaus subjektų lygmeniu operatyviai keistis informacija apie įvykusius kibernetinius incidentus ir jų sprendimą, diegimas.

Japonijos 2010 m. kibernetinio saugumo strategija[30] išsiskiria diegiamų informacijos saugumo priemonių, adaptuotų tiek viešajam ir privačiam sektoriams, tiek atskiriems vartotojams, įvairove. Strategijoje išskiriami trys esminiai tikslai (kryptys):

1) atviros, saugios ir patikimos kibernetinės erdvės sukūrimas;

2) sistemos, leidžiančios aktyviai reaguoti į sudėtingas ir įvairias kibernetines grėsmes sukūrimas ir įdiegimas;

3) priemonės, susijusios su 2011 m. kovo 11 d. įvykusio 9 balų stiprumo Rytų Japonijos žemės drebėjimo pasekmėmis[31].

---

[29] International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. White House, 2011. Prieiga: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[30] Prieiga internetu: https://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf

[31] Sukrečiantys skaičiai: žuvo arba dingo be žinios apie 24 000 žmonių, sugriauta apie 18 000 namų, 4,4 mln. namų ūkių liko be elektros, 1,5 mln. – be vandens. Šaltiniai internete: https://www.bbc.com/news/world-asia-pacific-12755739; https://www.britannica.com/event/Japan-earthquake-and-tsunami-of-2011/Aftermath-of-the-disaster

Tikslams įgyvendinti numatyta daugybė priemonių, tačiau visos jos aiškiai aprašytos, numatomi įgyvendinti veiksmai detalizuoti ir, kad ypač pagirtina, nustatyti atsakingi subjektai už kiekvienos priemonės kurio nors aspekto įgyvendinimą. Pvz., viena iš daugelio priemonių atvirai, saugiai ir patikimai kibernetinės erdvei kurti, yra įvairūs specializuoti mokymai. Mokymai strategijoje išskirstomi tiek pagal tematiką, tiek pagal juos išklausyti privalančias visuomenės grupes. Viena iš mokymų temų: apsauga nuo piktavališkų elektroninių laiškų, potencialiai galinčių pakenkti informacinių sistemų netrukdomam veikimui. Numatyti tiek mokymų organizatoriai, tiek juos išklausyti privalančių subjektų grupės, laikotarpis mokymų organizavimui, rezultatų pristatymui ir aptarimui.

Kibernetinio saugumo klausimai *Suomijoje* įtraukti į Saugumo strategiją, priimtą 2010 m. gruodžio 16 d.[32], jos preambulėje nurodant, kad kibernetinio saugumo užtikrinimas tapo nauju ir svarbiu iššūkiu valstybei, o kibernetinių incidentų, nukreiptų į telekomunikacijų ir informacines sistemas, pasekmės – vienos grėsmingiausių. Įdomu tai, kad Saugumo strategijoje pripažįstama, kad Suomijos teisės aktuose nėra įtvirtintos kibernetinių grėsmių sąvokos ir siūloma kibernetines grėsmes apibrėžti kaip pavojus, kylančius informacijos ir duomenų perdavimo tinklų saugumai, įskaitant telekomunikacijų tinklus, kompiuterines sistemas ir kritinės infrastruktūros valdymo įrenginius. Taip pat Saugumo strategijoje pateikiama pozicija, kuriai pritaria ir darbo autorius, kad saugios ir patikimos kibernetinės erdvės kūrimas neapsiriboja vien kova su kibernetiniais incidentais (pasekmėmis), būtina aktyvi prevencinė veikla. Saugumo strategijoje, kalbant apie kibernetinį saugumą, esminis akcentas tenka bendradarbiavimui.

Bendradarbiavimo įgyvendinimo atitinkamos priemonės (kartu su kitomis priemonėmis kibernetinio saugumo įgyvendinimui) numatytos Suomijos 2013 m. sausio 24 d. kibernetinio saugumo strategijoje. Strategijoje patraukliai pateikta Suomijos vizija kibernetinio saugumo srityje (Pavyzdys Nr. 4)[33]. Joje nurodoma, kad Suomija pajėgs apsaugoti gyvybiškai svarbią infrastruktūrą nuo kibernetinių grėsmių; valdžia, privataus verslo subjektai ir piliečiai naudotis saugia kibernetine erdve ir įgyvendins kibernetinio saugumo priemones tiek šalies, tiek tarptautiniu lygmeniu ir, keliamas itin ambicingas tikslas – iki 2016 m. tapti pirmaujančia šalimi, diegiant kibernetinio saugumo užtikrinimo priemones. Vizijos įgyvendinimui būtinas tarptautinis bendradarbiavimas, vidaus saugumas, gynybiniai pajėgumai, psichologinis atsparumas krizėms ir kiti pavyzdyje nurodyti elementai.

[32] Prieiga internetu: https://www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf
[33] Finnish National Cyber Security Strategy, 2013. Prieiga internete: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Finland

4 Pav. Suomijos kibernetinio saugumo vizija

Australijos 2009 m. kibernetinio saugumo strategijoje[34] tikslai (ateities vizija) formuluojami taip:

1. Gyventojai gebės išvengti kibernetinių grėsmių, apsaugoti savo naudojamą kompiuterinę techniką, taip pat tapatybę, privatumą ir finansus elektroninėje erdvėje;

2. Verslo subjektai naudos tik saugias ir atsparias informacines ir komunikacines technologijas ir užtikrins tiek vykdomų operacijų patikimumą, tiek vartotojų (klientų) duomenų saugumą;

3. Valdžios institucijos užtikrins naudojamų informacinių ir komunikacinių technologijų saugumą ir atsparumą[35].

Strategijoje numatyta steigti Australijos Kibernetinio saugumo operacijų centrą, kurio esminės funkcijos būtų šios: užtikrinti valstybinės reikšmės tinklų saugumą, identifikuoti sudėtingas kibernetines atakas, imtis prevencijos priemonių bei teikti pagalbą identifikuojant, neutralizuojant kibernetines atakas kritinės infrastruktūros objektuose, bendradarbiauti su privačiu sektoriumi, teikti konsultacijas. Centras buvo sėkmingai įsteigtas, vykdė jam deleguotas funkcijas kol 2014 m. jį pakeitė Australijos Kibernetinio saugumo centras[36], aktyviai bendradarbiaujantis su mokymo centrais, universitetais, privačiomis įmonėmis, taip pat rengiantis ir teikiantis įvairiausią informaciją kibernetinio saugumo klausimais: nuo nuotaikingų interaktyvių testų, iki detalių instrukcijų, padedančių atpažinti kibernetines grėsmes ir jų išvengti.

Įdomu tai, kad valstybių patirtį kuriant ir diegiant nacionalines kibernetinio saugumo strategijas analizavo Ekonominio Bendradarbiavimo ir Plėtros Organizacija. 2012 m. kibernetinio saugumo

[34] Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AGCyberSecurityStrategyforwebsite.pdf

[35] Būtina pažymėti, kad strategijos rengimo metu (2008 m.) kenkėjiškų programų, su kuriomis susidūrė interneto vartotojai Australijoje, skaičius siekė 17 692 567 (šaltinis: http://hoffmanmarcom.com/docs/Annual_Security_Threat_Report.pdf 19 p.), todėl tikslai vertintini kaip itin ambicingi.

[36] Daugiau informacijos: https://www.cyber.gov.au

strategijų tyrime analizuotos 10 valstybių kibernetinio saugumo strategijos, priimtos 2009 – 2011 m. (Australijos, Kanados, Prancūzijos, Vokietijos, Japonijos, Olandijos, Jungtinės Karalystės, Jungtinių Amerikos Valstijų, Suomijos ir Prancūzijos).

Pastebėta[37], kad daugumoje analizuotų strategijų aptariamas viešojo ir privataus sektorių bendradarbiavimas (kiek tai įgyvendinti leidžia strategijose numatytos priemonės – ginčytinas klausimas), koordinavimo funkcija priskiriama aukščiausiosioms valdžios institucijoms, plačiau ar siauriau reglamentuojamas tarptautinis bendradarbiavimas, akcentuojama pagarba fundamentaliosioms vertybėms: privatumui, laisvam informacijos judėjimui, saviraiškos laisvei ir kt. Kiti aspektai, išreikšti ne visose analizuotose strategijose, tačiau leidžiantys daryti išvadą dėl tendencijų reglamentuojant kibernetinio saugumo klausimus, būtų: lankstumas (jei gerai veikia savireguliacijos mechanizmai, galima apsieiti be reguliavimo priemonių nustatymo), ekonominių aspektų svarba (valstybių išlaidos kibernetinio saugumo priemonių diegimui auga) bei suvokimas, kad kibernetinio saugumo politikos įgyvendinime turi dalyvauti kuo platesnis subjektų ratas (ieškoma būdų įtraukti mokslo ir švietimo įstaigas, nevyriausybines organizacijas).

Analizuotų valstybių kibernetinio saugumo strategijų priemonių planuose ypatingas dėmesys skiriamas kritinės informacijos infrastruktūros[38] apsaugai, kovai su elektroniniais nusikaltimais, mokymosi ir švietimo svarbai, sąmoningumo skatinimui. Kitos reikšmingos priemonės: sektorių ir atskirų verslo subjektų, kurių pažeidžiamumas potencialiai sukeltų didžiausią žalą ekonomikai, identifikavimas; elektroninio identifikavimo ir realaus laiko stebėjimo sistemų vystymas; nepilnamečių apsaugos nuo žalingų poveikių internete priemonių diegimas; prekių ir produktų specialus ženklinimas; kibernetinio saugumo pratybos (tiek vykdomos valstybės viduje, tiek tarptautinės).

2.4 Vokietijos ir Prancūzijos nacionalinių kibernetinio saugumo strategijų lyginamoji analizė

Vokietija pagrįstai vertintina kaip valstybė, kurioje teisinis kibernetinio saugumo klausimų reglamentavimas itin išsamus ir nuoseklus. Dar 2011 m. vasario mėn. kibernetinio saugumo strategijoje buvo suformuluotos esminės kibernetinio saugumo klausimų sprendimo kryptys, detaliai reglamentuoti tarptautinio bendradarbiavimo klausimai, numatytos priemonės ypatingos svarbos informacinės infrastruktūros objektų apsaugai. Įgyvendinant šioje strategijoje numatytas priemones įsteigtas Nacionalinis kibernetinio saugumo reagavimo centras, koordinuojantis kibernetinių incidentų

[37] Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. OECD, 2012.
Prieiga internetu: https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[38] Kritinės informacijos infrastruktūros objektai teikia paslaugas, nuo kurių priklauso kertinės valstybės funkcijos. Jų nepasiekiamumas gali turėti skaudžių pasekmių visos visuomenės saugumui, ekonomikai ir gerbūviui. Šaltinis: The cost of incidents affecting CIIs. ENISA, August 2016. P. 4.

sprendimą ir užtikrinantis operatyvų keitimąsi aktualia informacija tarp visų suinteresuotų subjektų, bei Nacionalinė kibernetinio saugumo taryba, koordinuojanti prevencijos priemonių įgyvendinimą. Į Nacionalinės kibernetinio saugumo tarybos sudėti įtraukti verslo subjektų atstovai (asocijuoti nariai), akademinė bendruomenė (pagal poreikį). Kibernetinio saugumo klausimų sprendimas, įtraukiant suinteresuotus privataus sektoriaus subjektus ir naudojantis mokslinėmis žiniomis bei patirtimi, laikytinas pavyzdžiu kiekvienai valstybei, sprendžiančiai kibernetinio saugumo klausimus.

Šiuo metu Vokietijoje įgyvendinama 2016 m. lapkričio 7 d. patvirtinta kibernetinio saugumo strategija[39]. Dokumente nurodoma, kad Vokietijai iš esmės pavyko įgyvendinti 2011 m. strategijoje numatytas priemones, tačiau 2011 m. kelti tikslai, tokie kaip ypatingos svarbos informacinės infrastruktūros objektų apsauga, patikimų informacinių technologijų naudojimas, kova su nusikalstamomis veikomis elektroninėje erdvėje ir jų prevencija, reagavimo į kibernetines atakas įrankių kūrimas ir diegimas, išliko aktualūs. Kibernetinių incidentų skaičius nemažėja, jie tampa vis labiau komplikuoti, sunkiai nuspėjami ir paliečia visas visuomenės gyvenimo sritis.

Pagirtina, kad strategijoje neformuluojami deklaratyvūs ir sunkiai įgyvendinami tikslai, dar įžangoje nurodoma, kad „*toks reiškinys kaip šimtaprocentinis saugumas neegzistuoja“*, todėl tiek valdžios institucijos, tiek privataus sektoriaus subjektai turi siekti *pakankamo patikimumo* suvokiant, kad rizika išlieka visuomet.

Strategijoje iškeliami keturi esminiai siekiai (tikslai ir numatytos jų įgyvendinimo priemonės (30), Aptarsiu šiuos tikslus plačiau.

1. Saugumo ir autonomiško išsaugojimas skaitmeninėje aplinkoje. Pabrėžiama, kad tikslo įgyvendinimas neįmanomas be saugių ir patikimų informacinių technologijų, kurios turi būti prieinamos kiekvienam visuomenės nariui, nepriklausomai nuo jo veiklos sferos. Taip pat pripažįstama, kad vien tik to nepakanka, būtinas vartotojų suvokimas, kokie veiksmai leistini, kas kelia didžiausią riziką, koks elgesio modelis taikytinas konkrečiai situacijai. Įgyvendinant numatytą tikslą, orientuojamasi tiek į techninių standartų įgyvendinimą, tiek į visų amžiaus grupių vartotojų švietimą.

Esminės priemonės švietimo srityje*: visų vartotojų elektroninio raštingumo skatinimas ir informuotumo apie galimas rizikas didinimas* (saugaus elgesio elektroninėje erdvėje pagrindai įtraukiami į pradinio ir pagrindinio mokymo programas mokyklose, taip pat į studijų programas universitetuose, steigiami papildomi etatai universitetuose, bendradarbiaujama su privačiomis įmonėmis, ieškant galimybių papildomiems kursams, mokymo programoms ir pan.). Viena iš įdomesnių iniciatyvų – „Elektroninė kaimynystė“, siūlanti seminarus šalies mastu veikiančiuose kontaktiniuose punktuose, vadinamuose „DiNa-Treff“. Pirmasis „DiNa-Treff“ įsteigtas 2019 m. liepos

[39] Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Germany

3 d. Heidelberge[40]. Be seminarų, sudaromos ir kitos mokymosi galimybės, tokios kaip nemokamai platinami mokomieji vaizdo įrašai.

Esminės priemonės technologijų tobulinimo srityje: *sąlygų saugiai elektroninei komunikacijai kūrimas* (valstybė finansuoja mokslinius tyrimus ir iniciatyvas, padedančias kurti lengvą ir saugų šifravimą), *saugių elektroninių tapatybių kūrimas* (vartotojams suteikiama prieiga prie saugių, patogių naudoti ir šiuolaikiškų autentifikavimo priemonių internete, atsisakant ankstesnio standarto: vartotojo vardas/slaptažodis), *informacinių technologijų, atitinkančių saugumo standartus specialus ženklinimas, tyrimų informacinių technologijų saugumo srityje skatinimas* (išplėsta informacinių technologijų saugumo tyrimų programą „Nepriklausomas ir saugus skaitmeninis pasaulis 2015–2020“, stiprinami informacinių technologijų saugumo tyrimų kompetencijos centrų pajėgumai, siekiama įtraukti privataus verslo subjektus).

2. Jungtinės viešojo ir privataus sektorių pastangos. Suvokimas, kad tik visų suinteresuotų subjektų dalyvavimas kibernetinio saugumo kūrime ir įgyvendinime gali duoti gerus rezultatus, vertintinas kaip puikus pavyzdys. Kibernetinio saugumo strategijoje nurodoma, kad įmonės privalo gebėti apsaugoti nuo kibernetinių atakų tiek save, tiek klientus, tačiau ir valstybė turi imtis atitinkamų priemonių, apsaugodama visuomenei svarbius verslus. Dėl šios priežasties būtinas aktyvus, abipusiu pasitikėjimu grindžiamas bendradarbiavimas diegiant efektyvius informacinių technologijų saugumo standartus.

Esminės priemonės: *kritinės infrastruktūros apsauga, privataus verslo apsauga* (įmonėms, pasiekusioms nustatytus saugumo standartus, teikiama valstybės parama; bendradarbiavimas su privačiu sektoriumi ir moksline bendruomene plėtojant jau esamas iniciatyvas kibernetinio saugumo srityje: IT Sicherheit in der Wirtschaft (IT saugumas privačiame sektoriuje), Wirtschaftsschutz (Ekonominis saugumas) ir kt.), *informacinių technologijų sektoriaus stiprinimas* (informacinių technologijų prekių konkurencingumo didinimas, naudojant ženklinimą „IT saugumas, pagamintas Vokietijoje“, valstybės parama informacinių technologijų įmonėms), *keitimosi informacija apie kibernetines atakas ir jų prevenciją platformos sukūrimas ir įdiegimas* (platforma skirta tiek viešojo, tiek privataus sektorių subjektams).

3. Tvarios kibernetinio saugumo architektūros kūrimas, techniniai sprendimai. Nepaisant to, kad kibernetinio saugumo užtikrinimas laikoms valstybinės reikšmės užduotimi, įgyvendinant šį tikslą taip pat akcentuojamas privataus sektoriaus vaidmuo.

Esminės priemonės: *greitesnis ir efektyvesnis reagavimas į kibernetines grėsmes* (kuriamos mobiliosios reagavimo į kibernetinius incidentus komandos, veikiančios Nacionalinis kibernetinio saugumo reagavimo centro sudėtyje, vykstančios į kibernetinį išpuolį patyrusią įmonę ar valstybės

[40] Plačiau: https://www.sicher-im-netz.de/engagiert-aber-sicher-die-digitale-nachbarschaft-er%C3%B6ffnet-bundesweit-ersten-dina-treff-heidelberg

instituciją ir padedančios atkurti techninę veiklą. Taip pat numatyta Federaliniame kriminalinės policijos biure įsteigti specializuotą greitojo reagavimo padalinį, kuriame dirbtų kvalifikuoti informacinių technologijų ir žvalgybos specialistai, turintys patirties tiriant kibernetines atakas), *specialios kovos su kibernetiniu šnipinėjimu priemonės*, *išankstinio perspėjimo apie kibernetines atakas iš užsienio valstybių kūrimas ir diegimas, Saugumo institucijų informacinių technologijų centro įkūrimas* (šio centro užduotis – sukurti būtinus metodus, produktus ir strategijas, kuriuos savo veikloje naudotų saugumo institucijos. Pačiam centrui operatyvinių įgaliojimų nesuteikiama), *personalo kvalifikacijos tobulinimas* (numatoma dar glaudžiau bendradarbiauti su mokymo įstaigomis, kuriami atitinkami kursai ir mokymo modeliai aukštosiose mokyklose, be to, numatoma sudaryti galimybes įmonėms pagal poreikį keistis atitinkamų specialiųjų žinių turinčiais darbuotojais, prireikus spręsti specifinius kibernetinio saugumo klausimus).

Svarbu pažymėti ir tai, kad kibernetinio saugumo strategijoje numatyta plėsti Nacionalinio kibernetinio saugumo reagavimo centro ir Nacionalinės kibernetinio saugumo tarybos įgaliojimus. Nacionaliniam kibernetinio saugumo reagavimo centrui suteikiami įgaliojimai savarankiškai vertinti kibernetinius incidentus ir teikti ataskaitas apie kibernetinio saugumo būklę Vokietijoje. Be to, šis centras privalės skirti nemažai dėmesio mokymams ir pratyboms su visais suinteresuotais subjektais, neapsiribos vien tik dalijimusi informacija ir konsultacijomis. Nacionalinė kibernetinio saugumo taryba privalės numatyti ilgalaikes kibernetinio saugumo prevencinių priemonių įgyvendinimo tendencijas ir teikti kibernetinio saugumo priemonių siūlymus labiausiai pažeidžiamiems sektoriams ir reguliariai teikti rašytines ataskaitas Ministrų kabinetui.

4. Aktyvus vaidmuo formuojant kibernetinio saugumo politiką Europoje ir pasaulyje. Vokietijos Federalinio informacijos biuro patarėjas tarptautinių santykių klausimais S. Rothenpieler, 2017 m. balandžio 26 d. Atėnuose pristatydamas Vokietijos 2016 m. kibernetinio saugumo strategiją, pabrėžė, kad aiškus teisinis reglamentavimas, padidėjęs pasitikėjimas ir geresnis atsparumas kibernetiniams incidentams Europoje ir visame pasaulyje reiškia ir geresnį saugumą Vokietijoje. Dėl šios priežasties Vokietija ir toliau aktyviai dalyvaus kuriant kibernetinio saugumo politikos gaires[41].

Esminės priemonės: *aktyvus veiksmingos Europos kibernetinio saugumo politikos formavimas* (numatoma aktyviai įsitraukti į Europos Sąjungos bandomuosius teisinius ir techninius projektus, ypač, jei jie susiję su duomenų tvarkymu ir naudojimu, elektroninio identifikavimo priemonėmis, kvalifikuoto elektroninio parašo kūrimu), *aktyvus dalyvavimas plėtojant NATO kibernetinės gynybos politiką* (pabrėžiama, kad Vokietiją ypač domina hibridinės grėsmės), *tarptautinio kibernetinio saugumo formavimas* (tiek kuriant teisės aktus, formuluojant rekomendacijas, tiek dalyvaujant tarptautiniuose forumuose, diskusijose kibernetinio saugumo klausimais), *dvišalė ir regioninė parama*

[41] Prieiga internetu: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/april-2017/170426-bsi-enisa-nlo-presentation-v2.pdf

bei bendradarbiavimas stiprinant kibernetinius gebėjimus (akcentuojama parama kuriant ir diegiant patikimus ir atsparius informacinius tinklus, taip pat parama skaitmeninei infrastruktūrai šalyse partnerėse), *tarptautinės teisėsaugos stiprinimas* (intensyvus darbas kovoje su elektroniniais nusikaltimais, grėsmių prevencijos ir teisėsaugos sistemos tobulinimas).

Apibendrinant galima teigti, kad Vokietijos 2016 m. kibernetinio saugumo strategija išsiskiria:

1. Privataus sektoriaus vaidmens kuriant ir diegiant kibernetinio saugumo priemones suvokimu, bendradarbiavimu su privačiu sektoriumi ir šio sektoriaus subjektų įtraukimu į sprendimų kibernetinio saugumo srityje priėmimo procesą;

2. Pagarba mokslui, inovacijoms, akademinei bendruomenei. Puikiai suvokiama, kad be mokslo pažangos tikėtis gerų rezultatų kibernetinio saugumo srityje neįmanoma, todėl mokslas remiamas, o akademinės bendruomenės nariai įtraukiami į sprendimų priėmimo procesą. Be to ieškoma naujų ir inovatyvių būdų šviesti ir apmokyti saugaus elgesio pagrindų elektroninėje erdvėje visus visuomenės narius, tiek pradinių klasių moksleivius, tiek įmonių vadovus.

3. Itin aktyviu įsitraukimu į tarptautinės politikos kibernetinio saugumo srityje formavimą.

Prancūzija, kaip ir Vokietija, kibernetinio saugumo srityje jokiu būdu negali būti laikoma „pradinuke“ ar „antraeile žaidėja“. 2011 m. vasario mėn. Prancūzijos informacinių sistemų gynybos ir saugumo strategijoje[42] (priimtoje beveik tuo pat metu kaip ir Vokietijos 2011 m. vasario mėn. kibernetinio saugumo strategija) numatyti keturi tikslai: 1) pasaulinės galios kibernetinės gynybos srityje įgijimas; 2) gebėjimas priimti sprendimus, apsaugant informaciją, susijusią su šalies suverenitetu; 3) kritinės informacijos infrastruktūros apsauga; 4) elektroninės erdvės saugumo užtikrinimas. Tikslai įgyvendinami numatant atitinkamas priemones šiose veiklos sferose: prognozavimas ir analizė; grėsmių aptikimas ir reagavimas į jas; mokslinių, techninių galimybių bei žmogiškųjų gebėjimų stiprinimas; valstybės informacinių sistemų ir kritinės infrastruktūros objektų apsauga; teisėkūra; tarptautinis bendradarbiavimas; keitimasis informacija.

Strategijos preambulėje pabrėžiama saugios kibernetinės erdvės kūrimo svarba, kibernetinė erdvė prilyginama mūšio laukui ir naujajam Babelio bokštui – vietai, kurioje visos valstybės turėtų dalintis informacija ir idėjomis, tačiau realių, aiškių ir įgyvendinamų kibernetinio saugumo priemonių pasigendama. Įdomu tai, kad 2011 m. strategijoje pateikti esminių sąvokų, tokių kaip „kibernetinė erdvė“, „kibernetinis saugumas“, „kibernetinis nusikaltimas“, „kriptografija“ ir kitų apibrėžimai. Pvz., kibernetinis saugumas apibrėžiamas kaip siektina informacinės sistemos būsena, kai sistema atspari išorės įvykiams, galintiems pakenkti saugomų ir tvarkomų duomenų prieinamumui, vientisumui, konfidencialumui, taip pat ta sistema teikiamų paslaugų ar su jomis susijusių paslaugų prieinamumui.

[42] Prieiga internetu: https://www.enisa.europa.eu/media/news-tems/Information_system_security_France_strategy.pdf/view

Svarbu pažymėti ir tai, kad dar iki 2011 m. Informacinių sistemų gynybos ir saugumo strategijos priėmimo, 2009 m. liepos 7 d. įsteigta Tinklų ir informacijos saugumo agentūra, įdiegusi ir palaikanti „OpenCTI“ platformą, skirtą kibernetinės žvalgybos integravimui, informacijos apie potencialias grėsmes saugojimui, valdymui ir dalijimuisi ja[43]. Dabar „OpenCTI“ platformą valdo ne pelno siekianti organizacija „Luatix“. Tinklų ir informacijos saugumo agentūra yra „Luatix“ valdybos narė, ir toliau remianti platformos plėtrą.

Šiuo metu Prancūzijoje įgyvendinama 2015 m. spalio 10 d. Skaitmeninio saugumo strategija[44]. Prieš pradedant analizuoti dokumento turinį, būtina atkreipti dėmesį į tai, kad strategija vizualiai itin patraukliai pateikta, gausiai iliustruota, įžangoje pabrėžiama, kad kibernetinė erdvė tapo nesąžiningos konkurencijos ir šnipinėjimo veiklos lauku, kuriame tarpsta dezinformacija, propaganda, terorizmas ir nusikalstamumas. Kovojant su šiuo blogiu, būtinos sutelktos valstybės, privataus sektoriaus ir kiekvieno piliečio pastangos.

Aptarsiu 2015 m. strategijoje numatytus penkis strateginius tikslus ir priemones jiems įgyvendinti.

1. Valstybės informacinių sistemų ir kritinės infrastruktūros objektų apsauga. Tikslo įgyvendinimui numatytos penkios veiklos sferos.

Mokslinių ir techninių pajėgumų vystymas. Kuriama ekspertų grupė, į kurios sudėtį įtraukiami tiek ministerijų ir kitų valstybės institucijų, tokių kaip Generalinė investicijų komisija, Nacionalinė tyrimų agentūra ir kitos, atstovai, tiek mokslininkai ir verslininkai. Grupė vertina pradinius ir tęstinius švietimo poreikius, stebi mokslinius tyrimus ir teikia išvadas dėl jų plėtros, teikia siūlymus dėl konkrečių technologijų poreikio ir kasmet atsiskaito už savo veiklą tiesiogiai Ministrui Pirmininkui.

Technologijų saugumo stebėsenos diegimas. Strategijoje nenurodyta, kokių konkrečių veiksmų bus imtasi, tik pažymima apie reguliarų tikslinės bendruomenės informavimą apie saugų elgesį elektroninėje erdvėje.

Valstybės informacinių sistemų saugumo stipinimo spartinimas. Tai tęstiniai veiksmai, nes jau įgyvendinant 2011 m. strategiją buvo sukurtas tarpžinybinis elektroninių ryšių tinklas, įdiegti saugūs mobilieji terminalai. Dėl šios priežasties iš esmės reglamentuojamas tik ataskaitų apie saugumo būklę teikimas.

Pasirengimas plataus mąsto kibernetinio saugumo krizėms. Siekiant apsaugoti jautriausią informaciją numatomi pakeitimai vidaus teisės aktuose ir tinkamas TIS direktyvos nuostatų įgyvendinimas.

Autonomiško, įdiegtas vertybes atitinkančio, mąstymo būdo skatinimas. Itin specifinė priemonė, numatanti, kad nors informacinės technologijos skverbiasi į visas gyvenimo sritis, jos negali

[43] Plačiau: https://www.ssi.gouv.fr/en/

[44] Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=France

pakeisti jau susiformavusio požiūrio į fundamentalias vertybes, tokias kaip esminių teisių ir laisvių apsauga, valstybės suverenitetas, teritorijos neliečiamumas.

2. Saugi skaitmeninė erdvė, asmens duomenų ir privatumo apsauga, elektroninių nusikaltimų prevencija. Šio tikslo įgyvendinimo veiksmai apima tarpinstitucinį bendradarbiavimą teisėkūros ir techninių sprendimų diegimo srityje, taip pat teisinę ir techninę pagalbą nukentėjusiems nuo nusikaltimų elektroninėje erdvėje. Strategijoje pažymima, kad prancūzai iš esmės suvokia saugaus elgesio elektroninėje erdvėje reikalavimus, tačiau vis sunkiau atribojant profesinį gyvenimą nuo asmeninio ir visose gyvenimo srityse naudojantis ta pačia technologine įranga, kibernetinių išpuoliai gali sukelti tragiškų padarinių. Dėl itin didelio elektroninių nusikaltimų latentiškumo aukos dažnai negauna reikiamos pagalbos. Kita problema – gausėjantys dezinformacijos ir propagandos skleidimo atvejai. „*Skaitmeninėmis platformomis ir socialiniais tinklais pasinaudojama formuojant fundamentaliosioms Prancūzijos vertybėms prieštaraujančią nuomonę, o tai kenkia valstybės stabilumui“,* skelbiama 2015 m. strategijoje. Paminėsiu svarbesnes priemones, skirtas asmens duomenų ir privatumo apsaugai bei elektroninių nusikaltimų prevencijai įgyvendinti.

Fundamentaliųjų vertybių elektroninėje erdvėje apsauga. Įsteigta speciali informacinė platforma, skirta kovai su radikaliuoju islamizmu Stop-djiganizme.gouv.fr. Numatoma steigti kitas platformas, skirtas kovai su propaganda ir destabilizavimu.

Pagalba nukentėjusiems nuo elektroninių nusikaltimų. Numatyta sukurti specialią sistemą, kurioje nukentėję asmenys operatyviai ir, jiems pageidaujant, anonimiškai gautų konsultacijas ir rekomendacijas, taip pat realią techninę pagalbą (duomenų vagysčių, įsilaužimų, pakenkimo programinei įrangai atvejais).

Geresnė elektroninių nusikaltimų apskaita. Pasitelkiant atsakingas institucijas ir informacinių technologijų ekspertus ieškoma būdų ir priemonių į oficialią statistiką įtraukti kuo daugiau įvykdytų elektroninių nusikaltimų ir mažinti jų latentiškumą. Tam ypač naudinga jau minėta pagalbos nukentėjusiems nuo elektroninių nusikaltimų sistema.

Elektroninių tapatybių, privatumo ir asmens duomenų apsauga. Diegiamos sistemos, leidžiančios asmenims, naudojantis viena elektronine tapatybe, gauti skirtingas paslaugas.

Visiems prieinami techniniai sprendimai, padedantys saugiai jaustis elektroninėje erdvėje. Strategijoje numatyti techniniai sprendimai apima identifikavimo sistemas, specialų ženklinimą, išankstinį įspėjimą apie duomenų perdavimą tretiesiems asmenims.

3. Sąmoningumo kibernetinio saugumo srityje skatinimas, pradinis ir tęstinis švietimas. Pripažįstama, kad Prancūzija šioje srityje atsilieka, vaikų ir paauglių informuotumas apie saugų elgesį elektroninėje erdvėje nėra geras, o tai lemia itin dažną tapimą priekabiavimo ir patyčių internete aukomis. Taip pat pripažįstama, kad papildomi mokymai būtini ne tik jauniausiems elektroninės erdvės vartotojams, bet ir būsimiems skaitmeninių technologijų profesijų atstovams.

Esminės priemonės: *visų Prancūzijos gyventojų sąmoningumo kibernetinio saugumo srityje skatinimas* (kuriamos naujos ir tobulinamos jau įdiegtos ir gerų rezultatų pasiekusios programos, tokios kaip „Internet Licence“, teikianti konsultacijas studentams apie saugų elgesį internete, bei „Skaitmeninis švietimas visiems“, siūlanti seminarus ir konsultacijas kibernetinio saugumo srityje); *kibernetinio saugumo klausimų sprendimo įtraukimas į aukštojo ir tęstinio mokymo programas; kibernetinio saugumo pratybos, studijuojantiems informacines technologijas* (tęsiama 2013 m. „CyberEdu“ iniciatyva, kurios dėka kibernetinio saugumo klausimų sprendimas įtrauktas į informacinių technologijų programų studentų pirmųjų kursų studijas, taip pat numatomi specializuoti kibernetinio saugumo mokymai valstybės tarnautojams).

4. Saugi elektroninė aplinka versle ir pramonėje. Strategijoje pripažįstama, kad nemaža dalis Prancūzijoje gaminamos skaitmeninės įrangos ir teikiamų skaitmeninių paslaugų dar nepasiekė atitinkamo saugumo lygio. Skatinamas Prancūzijos gaminamų informacinių technologijų konkurencingumas, pasitelkiant specialų ženklinimą, skatinamos ir remiamos inovacijos, taip pat skatinamas viešojo ir privataus sektorių bendradarbiavimas.

Priemonės: *informacinių technologijų prekių ir paslaugų konkurencingumo skatinimas* (remiamos įmonės, kuriančios saugumo standartus atitinkančius informacinių technologijų produktus, finansuojami moksliniai tyrimai, nukreipti į aukšto lygio technologinio saugumo siūlymų teikimą), *bendradarbiavimas su privačiu sektoriumi* (teikiama pagalba (daugiausiai informacinė), diegiant saugumo sprendimus, saugumo standartus atitinkantys produktai atitinkamai ženklinami, laikomasi pozicijos, kad valstybės kišimasis į privataus sektoriaus veiklą būtinas tik susidūrus su rimta kibernetine ataka); *bendradarbiavimas su švietimo institucijomis, akademine bendruomene ir inovacijų centrais* (kuriamos rekomendacijos išankstinei saugumo rizikos analizei atlikti, produkto ar paslaugos patikimumo lygiui nustatyti); *kibernetinio saugumo reikalavimų integravimas elektroninėje erdvėje vykdant viešuosius pirkimus.*

5. Skaitmeninė strateginė autonomija, kibernetinės erdvės stabilumas. Strategijoje nurodoma, kad Prancūzija sieks stiprinti savo įtaką tarptautinėse organizacijose sprendžiant kibernetinio saugumo klausimus ir formuojant kibernetinio saugumo politiką, taip pat teiks paramą su didžiausiais saugumo iššūkiais susiduriančioms valstybėms. Tikslo įgyvendinimui numatytos šios trys priemonės:

Plano strateginei autonomijai įgyvendinti sukūrimas kartu su kitomis Europos Sąjungos valstybėmis narėmis (ypač didelis dėmesys standartizavimo ir sertifikavimo procedūroms, tyrimams informacinių technologijų sektoriuje, asmens duomenų apsaugai elektroninėje erdvėje, elektroninio susirašinėjimo tarp skirtingų valstybių šifravimui).

Įtakos stiprinimas sprendžiant kibernetinio saugumo klausimus ir dalyvaujant tarptautinėse diskusijose. Numatoma stiprinti bendradarbiavimą su visomis suinteresuotomis valstybėmis, taip pat

didinti investicijas neoficialiems tarptautiniams forumams, jungiantiems akademinės bendruomenės narius ir informacinių technologijų bei saugumo ekspertus.

Parama valstybėms, susiduriančioms su didžiausiais kibernetinio saugumo iššūkiais (ypač akcentuojama ypatingos svarbos infrastruktūros objektų apsauga ir kova su elektroniniais nusikaltimais).

Apibendrinant, galima suformuluoti šias išvadas:

1. Prancūzijos 2015 m. kibernetinio saugumo strategijoje akcentuojama būtinybė bendradarbiauti su privačiu sektoriumi, tačiau, skirtingai nei Vokietijos 2016 m. strategijoje, priemonių tam beveik nenumatyta. Apsiribojama informacijos teikimu, tam tikrais techniniais sprendimais (saugumo standartus atitinkančių produktų specialus ženklinimas), tačiau iš esmės laikomasi požiūrio, kad kol privati įmonė nesusidūrė su rimtu kibernetiniu incidentu, valstybės įsikišimas nereikalingas.

2. Numatytos priemonės kovai su elektroniniais nusikaltimais, jų latentiškumu vertintinos kaip geroji praktika. Autoriaus nuomone, ypač skatintinas būtų specialios platformos, kurioje nukentėję nuo nusikalstamų veikų kibernetinėje erdvėje subjektai galėtų gauti konsultacijas ir net realią techninę pagalbą, įdiegimas.

3. Didžiulės ambicijos ir noras įsitraukti į kibernetinio saugumo politikos formavimą tarptautiniu lygmeniu, tačiau jos nėra grindžiamos tokiomis aiškiai apibrėžtomis ir realiai įgyvendinamomis priemonėmis kaip Vokietijos 2016 m. strategijoje.

2.5 Jungtinių Amerikos Valstijų ir Jungtinės Karalystės patirtis, kuriant ir diegiant kibernetinio saugumo strategijas

Dar dvi valstybės, šiuo metu įgyvendinančios ne pirmąsias nacionalines kibernetinio saugumo strategijas ir turinčios nemažai patirties kibernetinio saugumo priemonių kūrimo ir diegimo procese, yra Jungtinės Amerikos Valstijos ir Jungtinė Karalystė.

Jungtinės Amerikos Valstijos (toliau – JAV) buvo pirmoji valstybė, ėmusi vertinti kibernetinį saugumą kaip sudėtinę nacionalinio saugumo dalį. Tai lėmė tiek informacinių technologijų ir elektroninės prekybos plėtra, tiek suvokimas, kad kibernetinis saugumas yra gyvybiškai svarbus energetikos (branduolinių jėgainių, dujų, elektros) infrastuktūroje bei transporto (metro, geležinkelio, oro) sistemose[45].

[45] A. Graželis „Kovų arena – kibernetinė erdvė“. Kibernetinio saugumo apžvalga, 2016 m., p. 21-24.

Nacionalinę kibernetinės erdvės saugumo strategiją[46] JAV priėmė 2003 m. 2015 m. buvo priimtas Pasidalijimo kibernetinio saugumo informacija įstatymas[47]. Tai didelės apimties (118 puslapių) dokumentas, susidedantis iš keturių skyrių: Dalijimasis informacija, Federacinis kibernetinis saugumas, Kibernetinio saugumo įgyvendinimas ir Kiti klausimai (aktualiausi privačiam sektoriui). Įstatyme akcentuojama dalijimosi informacija svarba, siekiama informaciją katalogizuoti ir padaryti prieinamą visiems suinteresuotiems subjektams. Šis teisės aktas sulaukė nemažai palaikymo ir pritarimo. Anot Israel Martinez, „Axon Global“ generalinio prezidento ir direktoriaus, „tai galingas įrankis, kuris suderina viešojo ir privataus sektoriaus interesus, kuriant saugią kibernetinę ekosistemą“[48].

2011 m. JAV kibernetinio saugumo strategija jau buvo trumpai aptarta šio darbo 2.1 poskyryje „Pirmosios nacionalinės kibernetinio saugumo strategijos, jų turinio esminiai aspektai“. Šiuo metu JAV įgyvendina 2018 m. rugsėjo mėn. priimtą kibernetinio saugumo strategiją[49]. Strategija patraukliai pateikta, su iliustracijomis, palikta erdvės kiekvieno skaitytojo asmeniniams užrašams, skatinanti patriotizmą, pradedama Prezidento žodžiu ir jo įsipareigojimais užtikrinti tinklų, sistemų ir duomenų saugumą. Taip pat pateiktas istorinis ekskursas, išsamiai paaiškinta, kodėl strategija buvo priimta. Dokumento apimtis – 40 puslapių, tačiau būtina įvertinti tai, kad dalį jų užima iliustracijos ir erdvė skaitytojo pastaboms ir komentarams.

Prezidento įžanginiame žodyje prisiimami šie JAV įsipareigojimai kibernetinėje erdvėje:

1) saugoti tinklus sistemas ir duomenis, šią apsaugą vertinant visos valstybės saugumo mastu;

2) skatinti ir palaikyti valstybės klestėjimą, puoselėjant saugią kibernetinę erdvę ir diegiant inovacijas;

3) užtikrinti taiką ir saugumą, atgrasant nuo naudojimosi kibernetine erdve piktybiniais tikslais ir baudžiant už tai;

4) įgyvendinant kibernetinio saugumo priemones, plėsti JAV įtaką pasaulyje.

Pastebėtina, kad strategijos tekstas, ne vien jos įžanga, skatina patriotiškumą, kviečia veikti kartu, skatina palaikyti amerikietiškąją kultūrą.

Strategijos turinį sudaro keturių tikslų nurodymas, kiekvieno jų įgyvendinimui numatytų priemonių ir veiksmų joms įgyvendinti išvardijimas. Aptarsiu juos plačiau.

1. Saugoti piliečius, Tėvynę, gyvenimo būdą (tradicijas). Siekį numatoma įgyvendinti per nacionalinių tinklų, informacijos ir kritinės infrastruktūros apsaugą, kovą su elektroniniais

[46] National Strategy to Secure Cyberspace, 2003. Prieiga internetu: https://georgewbush-whitehouse.archives.gov/pcipb/cyberspace_strategy.pdf

[47] Cybersecurity Information Sharing Act, 2015. Prieiga internetu: https://www.congress.gov/114/bills/s754/BILLS-114s754es.pdf

[48] Cybersecurity Act of 2015 review. What it Means for Cybersecurity Governance and Enterprise Risk Management. Joseph J. Panetta & R. Andrew Schroth. Kogod School of Business, Washington, 2015.

[49] Prieiga internetu: https://trummpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

nusikaltimais. Veiksmai, numatyti atskiroms priemonėms įgyvendinti, įvardijami konkrečiai ir aiškiai, be to, strategijoje įvardijama, kas konkrečiai atsako už atitinkamos priemonės įgyvendinimą.

Siekiant apsaugoti nacionalinius tinklus ir informaciją, numatoma *įdiegti centralizuoto valdymo su vieningu dalijimusi informacija sistemą*, skatinamas inovacijų diegimas. Siekiant užtikrinti efektyvią kritinės infrastruktūros apsaugą, numatomas aiškus pasiskirstymas atsakomybe tarp viešojo ir privataus sektorių subjektų, išskiriamos sritys, kurioms suteikiamas prioritetas, mažinant rizikas: nacionalinis saugumas, energetika, bankininkystė ir finansai, sveikata ir socialinė apsauga, viešieji ryšiai, informacinės technologijos, transportas. Pabrėžiama *mokymų ir švietimo svarba*, skatinamas naujų kibernetinio saugumo priemonių diegimas. Siekiant užkirsti kelią kibernetinėje erdvėje vykdomoms nusikalstamoms veikoms, numatoma tiek skatinti pranešti apie bet kokio pobūdžio kibernetinius incidentus, tiek nedelsiant į juos reaguoti. Taip pat numatoma tobulinti teisės aktus, reglamentuojančius neleistinų kibernetinėje erdvėje veiksmų kriminalizavimą, modernizuoti teisės aktus, skirtus kovai su organizuotais nusikaltimais elektroninėje erdvėje, plėsti ir stiprinti tarptautinį bendradarbiavimą.

2. Skatinti šalies klestėjimą. Strategijoje patikslinama, kad klestėjimas nagrinėjamu atveju siejamas su JAV įtakos informacinių technologijų plėtros sferoje išsaugojimu, saugios kibernetinės erdvės sukūrimu ir palaikymu, ekonomikos plėtra ir inovacijų diegimu. Siekiant šio tikslo akcentuojamas aukštos kvalifikacijos informacinių technologijų ir saugumo *specialistų rengimas*, *investicijų inovacijoms ir išradimams būtinybė*, taip pat būtinybė nuolat peržiūrėti ir atnaujinti informacinių technologijų standartus. Pagirtina, kad nemažai dėmesio skiriama intelektinės nuosavybės apsaugos priemonėms, siekiu naudojimąsi informacinėmis technologijoms padaryti lengvai prieinamą visoms visuomenės grupėms. Kritiškiau vertintina tokia priemonė kaip darbuotojų švietimas ir perkvalifikavimas, kuri iš esmės yra gera, tačiau turi silpnas sąsajas su kibernetinio saugumo užtikrinimu.

3. Užtikrinti taiką per galią (elgesio normų nustatymas, nepriimtino elgesio kibernetinėje erdvėje ir pasekmių už jį apibrėžimas). Strategijoje numatoma atitinkamų operatyvinių veiksmų reglamentavimas ir taikymo ribų nustatymas, siekis, kad pasekmės už kenkėjiškus veiksmus kibernetinėje erdvėje būtų neišvengiamos.

4. Stiprinti įtaką pasaulyje. To siekiama užtikrinant visiems atvirą ir saugią elektroninę erdvę bei stiprinant gebėjimus kibernetinio saugumo srityje.

Pastebima, kad per strategijoje numatytas priemones vyksta aktyvus bendradarbiavimas su privataus verslo subjektais, Vyriausybei prisiimant nemažą dalį atsakomybės už privataus sektoriaus subjektų naudojamų informacinių technologijų saugumą. Be to beveik kiekviename kibernetinio saugumo strategijos skyriuje pabrėžiama, kad saugios kibernetinės erdvės sukūrimas ir kibernetinio saugumo priemonių įgyvendinimas priklauso nuo privataus sektoriaus paramos. Taip pat nurodoma,

kad privataus sektoriaus subjektai privalo teikti paramą teisėsaugos institucijoms, padedant nustatyti nusikalstamas veikas kibernetinėje erdvėje vykdančius asmenis ir atskleisti tas veikas, kas sukelia nemažai problemų įmonėms, griežtai besilaikančioms asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimų[50].

Kritikos sulaukia ir realios galimybės įgyvendinti kibernetinio saugumo strategijoje numatytas, šiek tiek deklaratyviai skambančias priemones, todėl, manyčiau, teisingai pasisakoma apie būtinybę ieškoti balanso tarp visiško atvirumo ir visiško saugumo.

Pagrindus kibernetinio saugumo stiprinimui Jungtinė Karalystė suformulavo 2011 m. lapkričio mėn. patvirtintoje Apsaugos ir palaikymo skaitmeniniame pasaulyje strategijoje[51], nurodydama aiškią viziją: „*iki 2015 m. iš energingos ir saugios elektroninės erdvės gauti ekonominę ir socialinę vertę, kuriai esant valstybės veiksmai, įgyvendinant pamatines vertybes, teisingumą, skaidrumą ir įstatymų galią, didins gerovę, nacionalinį saugumą ir formuos tvirtą visuomenę“.* Vizijos įgyvendinimui suformuluoti šie tikslai: 1) kovoti su elektroniniais nusikaltimais ir tapti viena saugiausių pasaulyje šalių verslui elektroninėje erdvėje vystyti; 2) didinti atsparumą kibernetiniams išpuoliams ir apsaugoti savo interesus kibernetinėje erdvėje; 3) suformuoti atvirą ir stabilią elektroninę erdvę, kuria saugiai naudotųsi kiekvienas visuomenės narys; 4) žinių, įgūdžių ir gebėjimų, leidžiančių užtikrinti kibernetinės erdvės saugumą, stipinimas.

Tikslų įgyvendinimo rezultatai aprašyti šiuo metu įgyvendinamoje Jungtinės Karalystės kibernetinio saugumo strategijoje 2016–2021 metams, priimtoje 2016 m. lapkričio 29 d.[52]. Strategijoje nurodoma, kad 2011 m. strategijos įgyvendinimas valstybei kainavo 860 mln. svarų sterlingų, pasiekta ženklių rezultatų kibernetinio saugumo srityje, tačiau sudėtingėjant kibernetinėms grėsmėms ir sunkėjant kibernetinių išpuolių pasekmėms „*sustoti ne tik negalima, bet ir pavojinga“*.

2016 m. strategijos turinys išsiskiria iš anksčiau analizuotų strategijų turinio ir, autoriaus manymu, būtų labiausiai rekomenduotinas tiek Lietuvai, tobulint galiojančią ir rengiant naują kibernetinio saugumo strategiją, tiek kitoms valstybėms – vis dar žengiančioms pirmuosius kibernetinio saugumo priemonių įgyvendinimo žingsnius ar atvirkščiai, jau turinčioms nemažai patirties šioje srityje.

Strategija neapsiriboja preambule, trumpa ataskaita apie ankstesnėje strategijoje numatytų priemonių įgyvendinimą, tikslų nurodymu ir jų įgyvendinimui skirtų priemonių aprašymu, ji daug platesnė. **Vizija**, kuri turi būti įgyvendinta iki 2021 m. įskaitytinai, šiek tiek kuklesnė, nei 2011 m.

---

[50] U. S. National Cyber Strategy: What you need to know. Anastasios Arampatzis, 2018. Prieiga internetu: https://www.tripwire.com/state-of-security/government/us-cyber-strategy/

[51] UK cybersecurity strategy. Protecting and promoting the UK in a digital world. Prieiga internetu: https://www.gov.uk/government/publications/cyber-security-strategy

[52] Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=United%20Kingdom

strategijoje numatyta – Jungtinė Karalystė privalo išlikti saugi ir atspari kibernetinėms grėsmėms, o jos elektroninė erdvė – klestinti ir patikima. Biudžetas kibernetinio saugumo priemonių įgyvendinimui ženkliai auga, numatyta tam skirti 1,9 bln. svarų sterlingų.

Strategijoje pateikiama *kibernetinio saugumo* sąvoka, – tai informacinių sistemų (techninės ir programinės įrangos ir su jomis susijusios struktūros) ir jose esančių duomenų apsauga nuo neteisėtos prieigos, atskleidimo ar praradimo)[53].

Atskiras skyrius strategijoje skiriamas grėsmių ir pažeidžiamumų įvardijimui. Išskiriamos šios **grėsmės:** 1) *kibernetiniai nusikaltimai* (vykdomi pasinaudojant informacinėmis technologijomis, kai tos technologijos yra nusikaltimo įrankis arba objektas (pvz., kenkėjiškų programų platinimas. Siekiant finansinės naudos), taip pat įprastiniai nusikaltimai, kurių pasekmės dėl naudojimosi informacinėmis technologijomis sunkėja (pvz., sukčiavimas ir duomenų vagystė); 2) *kitų valstybių remiamos grėsmės*, nukreiptos į jautriausius sektorius, tokius kaip gynyba, finansai, energetika, telekomunikacijos; 3) *terorizmas*[54]*;* 4) *haktyvizmas*[55]*;* 5) *script kiddies* (programišiai, naudojantys kitų sukurtą įrangą kibernetiniams įsilaužimams).

Pažeidžiamumai: 1) *besiplečiantis naudojamos informacinių technologijų įrangos skaičius* (neapsiribojama stacionariu at nešiojamuoju kompiuteriu, vienas asmuo naudojasi keletu įrangos objektų, plečiasi daiktų internetas, todėl galimybių nukentėti nuo kibernetinių incidentų daugėja); 2) *prastas kibernetinės higienos laikymasis* (kuo labiau pažeidžiama potenciali auka, tuo mažiau pastangų reikia potencialiam užpuolikui); 3) *nepakankami gebėjimai ir specializuotų mokymų trūkumas* (pabrėžiama, kad kvalifikuotų specialistų trūksta tiek valstybiniame, tiek privačiame sektoriuje); 4) *pasenusios ir reguliariai neatnaujinamos informacinės sistemos* (nemažai svarbias funkcijas vykdančių institucijų ir organizacijų naudojasi programine įranga, nesuderinama su būtinais atnaujinimais[56]); 5) *įsilaužimo išteklių prieinamumas* (internete nesunkiai prieinama informacija apie tai, kaip įsilaužti į konkrečią sistemą, pakenkti konkrečiai programinei įrangai ir pan.).

Įvertinus didžiausias kibernetinio saugumo grėsmes ir pažeidžiamumus strategijoje suformuluoti atskiri tikslai ir atsakomybės valstybei, privačiam ir viešajam sektoriui bei gyventojams.

Valstybė turėtų ginti šalį nuo kitų valstybių išpuolių kibernetinėje erdvėje ir taip apsaugoti piliečių teises ir laisves, ekonomiką. Taip pat valstybė privalo kurti ir diegti duomenų apsaugos priemones visos šalies mastu, suformuluoti aiškias ir visiems suprantamas saugaus elgesio

[53] Apima ir sistemos operatorių tyčinius veiksmus ar sąmoningą saugumo procedūrų nesilaikymą.
[54] Įdomu tai, kad Jungtinė Karalystė kibernetinių teroristų techninį lygį vertina kaip sąlyginai žemą, tačiau pripažįsta, kad jų atakos elektroninėje erdvėje tapo pernelyg dažnos, todėl be papildomų saugumo priemonių išsiversti nesitikima.
[55] Haktyvizmas – tai internetinis judėjimas, tam tikromis veiklomis kompiuteriais ir kompiuterių tinklais siekiantis įvairių tikslų. Ši veikla gali pasiekti panašius tikslus kaip protestai, aktyvizmas ar pilietinis nepaklusnumas. Šaltinis: wikipedia: https://lt.wikipedia.org/wiki/Haktyvistai
[56] Šokiruojantys skaičiai: iš 115 000 patikrintų Cisco Systems įrenginių, 106 000 naudojo pažeistą programinę įrangą. Šaltinis internete: https://www.coursehero.com/file/p6gf0vg/cyber-incidents-affecting-governments-and-corporations-Cyber-attacks-are-not/

kibernetinėje erdvėje taisykles, nustatyti saugumo standartus, privalomus visoms įmonėms ir organizacijoms. Valstybė prisiima atsakomybę už kritinės infrastruktūros objektų apsaugą.

Privataus ir viešojo sektoriaus subjektai privalo tinkamai tvarkyti asmens duomenis, užtikrinti saugų paslaugų teikimą, naudotis tik saugomo standartus atitinkančia įranga, suvokti potencialias kibernetines grėsmes ir gebėti prisiimti atsakomybę už jų pasekmes.

Iš gyventojų reikalaujama prisiimti asmeninę atsakomybę už sąmoningą saugumo reikalavimų ir standartų elektroninėje erdvėje nesilaikymą.

Tikslai Jungtinės Karalystės kibernetinio saugumo strategijoje formuluojami kaip „pokyčių reikalaujančios veiklos sritys“. Tokių išskiriama dvi: pokyčiai rinkoje ir Vyriausybės funkcijų plėtimas. Elektroniniu būdu vykdomas verslas, elektroninė rinka nėra pakankamai saugu, nepaisant investicijų ir pastangų, įgyvendinant 2011 m. strategijoje numatytas priemones. Būtinas papildomų techninių priemonių diegimas ir švietimas kibernetinio saugumo klausimais.

Iš Vyriausybės reikalaujama glaudesnio ir aktyvesnio bendradarbiavimo su privačiu sektoriumi skatinimo, taip pat veiksmų sutelkimo į šias sritis: paramą švietimui, inovacijoms, moksliniams tyrimams; žvalgybą, siekiant kuo greičiau identifikuoti potencialias kibernetines atakas; techninių priemonių kūrimą ir diegimą; Nacionalinio kibernetinio saugumo centro veiklos plėtrą. Paskutinioji sritis reikalauja detalesnio paaiškinimo. Nacionalinis kibernetinio saugumo centras Jungtinėje Karalystėje įsteigtas 2016 m. spalio 1 d[57]. Esminė jo funkcija – pagalba ir konsultacijos viešojo ir privataus sektoriaus subjektams ar atskiriems individams susidūrus su kibernetiniais incidentais. Vadovaujantis 2016 m. strategija, Nacionalinis kibernetinio saugumo centras prisiima atsakomybę už stambaus masto kibernetinių incidentų tyrimą, nustato būdus ir priemones operatyviam keitimuisi informacija apie kibernetinius incidentus tarp visų suinteresuotų subjektų bei teikia kvalifikuotą pagalba ypatingos svarbos sektoriams (finansų, energetikos, telekomunikacijų ir kt.).

Kibernetinio saugumo užtikrinimo priemonės pateikiamos strategijos įgyvendinimo programoje, kiekvienai nurodytų priemonių grupių priskiriant vieną iš keturių esminių paskirčių: gynyba (reagavimas į kibernetinius incidentus), atgrasymas (prevenciniai veiksmai, nukreipti į potencialias kibernetines grėsmes), vystymas (mokslinių tyrimų plėtra) ir tarptautinis bendradarbiavimas.

Gynybos paskirčiai priskirtos šios priemonės: *veiksmingas reagavimas į kibernetinius incidentus* (skatinimas pranešti apie įvykusius incidentus, Nacionalinio kibernetinio saugumo centro funkcijų plėtimas, kibernetinių incidentų priežasčių identifikavimas ir prevencinių priemonių taikymas); *bendradarbiavimas su privačiu sektoriumi, taikant technines saugo priemones, saugumo standartus atitinkančių produktų kūrimas ir paslaugų teikimas, saugesnio interneto kūrimas* (parama įmonėms, kuriančioms saugumo standartus atitinkančius produktus, naujų autentifikavimo

[57] Plačiau apie centro veiklą: https://www.ncsc.gov.uk/

mechanizmų kūrimas ir diegimas, investavimas į antivirusines programas); *valstybės informacinių sistemų apsauga; kritinės infrastruktūros objektų apsauga; privataus sektoriaus ir visuomenės elgsenos modelių keitimas (*skatinamas sąmoningumas ir esminių elgesio standartų, padedančių apsisaugoti patiems, apsaugoti savo verslą ir klientus, suvokimas).

Priemonės, priskirtos atgrasymo paskirčiai: *kova su kibernetiniu nusikalstamumu, elektroninių nusikaltimų skaičiaus mažinimas* (bendradarbiaujama su Nacionaliniu kibernetinio saugumo centru, dalijamasi gerąja patirtimi su užsienio partneriais, kuriama 24/7 platforma, sudaranti galimybę pranešti apie elektroninius nusikaltimus visą parą ir gauti būtinas konsultacijas ir pagalbą); *kova su užsienio valstybių kibernetinėmis atakomis* (ieškoma būdų kuo efektyviau įgyvendinti tarptautines konvencijas, dvišalius ir daugiašalius susitarimus, kolektyvinės gynybos ir bendradarbiavimo skatinimas); *terorizmo prevencija* (taip pat akcentuojamas tarptautinis bendradarbiavimas); *kriptografijos galimybių pritaikymas* (labiausiai orientuota į valstybės paslaptimis laikomos informacijos apsaugą).

Vystymo paskirčiai strategijoje priskirtos šios priemonės: *gebėjimu kibernetinio saugumo srityje stiprinimas* (kibernetinio saugumo klausimų programos įtraukiamos į švietimo sistemą, diegiamos specialios disciplinos informacinių technologijų studentams, bendradarbiaujama su akademine bendruomene, profesinėmis organizacijomis, be to, organizuojamos specializuotos pratybos jautrių sektorių darbuotojams); *inovacijų kibernetinio saugumo sektoriuje skatinimas* (steigiami specialūs paramos fondai, įmonėms sudaromos galimybės kurti ir testuoti bandomuosius produktus, tokios pastangos finansiškai skatinamos ir palaikomos); *kibernetinio saugumo mokslo ir technologijų plėtra* (kuriamos specialios doktorantūros studijų programos, finansuojami moksliniai tyrimai).

Tarptautinio bendradarbiavimo srityje ketinama ir toliau glaudžiai bendradarbiauti su užsienio valstybėmis, kuriant saugią ir patikimą kibernetinę erdvę, aktyviai dalyvauti formuojant tarptautinę kibernetinio saugumo politiką. Jungtinė Karalystė ypač akcentuoja bendradarbiavimo tarptautinės baudžiamosios teisės srityje būtinybę, ieškant naujų efektyvių būdų kovai su elektroniniais nusikaltimais.

Apibendrinant Jungtinės Karalystės kibernetinio saugumo strategiją darytinos šios išvados:

1. Strategijos struktūra ir informacijos pateikimas – daugeliui valstybių sektinas pavyzdys. Strategija išsami, teisinis reglamentavimas aiškus ir suprantamas, skirtingai nuo kitų analizuotų valstybių strategijų, joje nėra deklaratyvių, neįgyvendinamų tikslų. Be to, informacija pateikiama itin patraukliai, su įsimintinomis citatomis, kibernetinių incidentų pavyzdžiais.

2. Visų pirma strategijoje akcentuojamos grėsmės, problemos, pažeidžiamumai kibernetinio saugumo srityje, o tik po nurodomos priemonės, padėsiančios tas problemas spręsti. Priemonių planas nesudėtingas, be to, jame pateikiami numatytų įgyvendinti priemonių veiksmingumo vertinimo kriterijai.

3. Nemažai dėmesio skiriama švietimo kibernetinio saugumo srityje poreikiui, tačiau švietimas, skirtingai nei Vokietijoje ar Prancūzijoje, orientuotas į aukštąjį mokslą, doktorantus, taip pat informacinių technologijų studentus.

4. Daug dėmesio skiriama ir nusikaltimų elektroninėje erdvėje tyrimui ir prevencijai. Ieškoma tiek mokslinių, tiek techninių prevencijos būdų, puikiai suvokiama tarptautinio bendradarbiavimo, efektyvaus tarptautinių susitarimų įgyvendinimo reikšmė.

2.6 Kinijos, Pietų Korėjos ir Australijos kibernetinio saugumo strategijų palyginimas

Kinijos, Pietų Korėjos ir Australijos požiūriai į kibernetinio saugumo problemų sprendimą skiriasi, vis tik šių valstybių kibernetinio saugumo strateginiuose dokumentuose galime pastebėti labai panašių aspektų.

Šiuo metu Kinija įgyvendina 2016 m. gruodžio 27 d. priimtą kibernetinio saugumo strategiją[58]. Dokumento apimtis apie 7 puslapius (vertimas į anglų kalbą). Pažymėtina, kad šiame darbe pateikiamas tik ribotas strategijos struktūros ir jos turinio vertinimas, nes viešai prieinamas ir publikuojamas tik neoficialus strategijos vertimas iš kinų į anglų kalbą. Įdomus ir tas faktas, kad kinų kalboje nevartojamas terminas „kibernetinis saugumas“, naudojamasi šio termino atitikmenimis[59].

Strategijoje aiškiai išskirti principai, tikslai ir strateginės užduotys. Nurodomi šie **principai**:

1) suvereniteto elektroninėje erdvėje gynyba;

2) taikus elektroninės erdvės naudojimas;

3) elektroninės erdvės valdymas pagal įstatymus;

4) visapusiškas kibernetinio saugumo ir jo plėtros valdymas.

Pristatant principus 2016 m. kibernetinio saugumo strategijoje pabrėžiama, kad elektroninė erdvė yra naujoji tautos suvereniteto teritorija. Suverenitetas suvokiamas kaip visiškas politinis ir teisinis valstybės savarankiškumas, jos nepriklausomybė. Strategijoje numatyta **vizija** įgyvendinti novatorišką, koordinuotą, ekologišką, atvirą ir bendrą plėtros koncepciją; stiprinti sąmoningumą rizikos ir krizių srityse; suplanuoti ir įgyvendinti dviejų esminių saugumo klausimų – vidaus ir išorės saugumo – plėtrą; efektyviai gintis, skatinti taiką, saugumą, atvirumą, bendradarbiavimą ir tvarką elektroninėje erdvėje; ginti nacionalinio suvereniteto, saugumo ir plėtros interesus bei įgyvendinti esminį strateginį tikslą – sukurti stiprią kibernetinę galią.

[58] Neoficialaus dokumento vertimo prieiga internetu: https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

[59] Warring State: Chinas Cybersecurity Strategy. Amy Chang, Center for a New American Security, 2014. P.13.

Kibernetinio saugumo strategijoje nurodomi šie **tikslai**[60]:

1. Tvarka I: veiksminga kova su piktnaudžiavimu informacinėmis technologijomis, ginklavimosi elektroninėje erdvėje kontrolė, efektyvus galimybių kilti konfliktams elektroninėje erdvėje užkirtimas;

2. Saugumas, apimantis kibernetinio saugumo rizikų kontrolę, nacionalinių kibernetinio saugumo apsaugos sistemų tobulinimą, informacinių ir komunikacinių technologijų ir įrangos saugumo užtikrinimą;

3. Atvirumas I : informacinių technologijų saugumo standartų laikymasis, elektroninių rinkų atvirumas ir skaidrumas, skaitmeninės atskirties mažinimas, t. y. neturi būti išskiriami dideli ir maži, stiprūs ir silpni, turtingi ir neturtingi. Visos pasaulio valstybės, ypač besivystančios, turi turėti galimybę pasidalinti plėtros pasiekimais, vystymosi rezultatais ir sąžiningai dalyvauti elektroninės erdvės valdyme;

4. Atvirumas II: visos pasaulio šalys turi plėtoti glaudesnį bendradarbiavimą informacinių ir komunikacinių technologijų mainų, kibernetinio terorizmo ir nusikalstamų veikų kibernetinėje erdvėje užkardymo procese;

5. Tvarka II: visapusiška visuomenės teisės žinoti ir teisės reikšti nuomonę gynyba. Visapusiška pagarba žmogaus teisėms ir asmens privatumo elektroninėje erdvėje apsauga.

Autoriaus nuomone, realus išsikeltų tikslų įgyvendinimas kelia pagrįstų abejonių, nes jie orientuoti ne tik į pačią valstybę, bet ir į kitų valstybių veiksmus ir pastangas užtikrinant kibernetinį saugumą. Tikslai abstraktūs, pakankamai platūs, nors siekis padėti besivystančioms šalims kibernetinio saugumo srityje vertintinas teigiamai.

Strateginės užduotys Kinijos kibernetinio saugumo strategijoje:

1. *Ginti kibernetinės erdvės suverenitetą.* Patikslinama, kad suvereniteto gynybai būtinas Konstitucijos, įstatymų i kitų teisės aktų laikymasis, taip pat nurodoma, kad bus imtasi visų priemonių, įskaitant ekonomines, administracines, mokslo, technologines, teisines, diplomatines ir karines (įdomus aspektas, atsižvelgiant į tai, kad vienas esminių strategijos principų yra taikus elektroninės erdvės naudojimas), siekiant palaikyti šalies suverenitetą elektroninėje erdvėje.

2. *Užtikrinti nacionalinį saugumą:* užkirsti kelią ir bausti už bet kokius veiksmus, susijusius su kibernetinio saugumo pažeidimais, siekiančiais kurstyti separatizmą ar maištą, skatinančiais režimo nuvertimą.

3. *Apsaugoti ypatingos svarbos informacijos infrastruktūrą:* imtis visų įmanomų priemonių kritinės informacijos infrastruktūrai ir jos duomenims apsaugoti nuo užpuolimo ar sunaikinimo. Sukurti kibernetinio saugumo informacijos mainų mechanizmus Vyriausybėje, atskiruose jos sektoriuose ir įmonėse.

[60] Tikslai įvardyti taip, kaip jie įvardyti Kinijos kibernetinio saugumo strategijos vertime į anglų kalbą.

Įdomu tai, kad įgyvendinant nurodytą strateginę užduotį numatyta atsisakyti privačių įmonių vaidmens, saugant ypatingos svarbos informacinę infrastruktūrą.

4. *Kurti sveiką internetinę kultūrą:* plėtoti pozityvią internetinę kultūrą, skatinti naujų verslų plėtrą ir naujų produktų kūrimą. Taip pat numatyta įdiegti kinų kultūros sklaidos internete projektą, skatinantį tiek tradicinės, tiek šiuolaikinės kinų kultūros šedevrų skaitmeninimą ir sklaidą.

5. *Kovoti su elektroniniais nusikaltimais, šnipinėjimu ir terorizmu.* Įgyvendinant šią užduoti numatyta imtis griežtų priemonių prieš internetinį sukčiavimą, vagystes, prekybą narkotinėmis medžiagomis ir ginklais elektroninėje erdvėje, kėsinimąsi į piliečių asmeninę informaciją, nepadorumo ir sekso skatinimą, intelektinės nuosavybės teisių pažeidimus.

6. *Tobulinti kibernetinio saugumo valdymo sistemą.* Sistemos tobulinimas įgyvendinamas tiek kuriant teisinę bazę (numatyta parengti ir paskelbti Kibernetinio saugumo įstatymą, Nepilnamečių apsaugos elektroninėje erdvėje nuostatus, kitus teisės aktus, peržiūrėti galiojančius teisės aktus), tiek vykdant kitas priemones: stiprinant telekomunikacijų, žodžio laisvės, komercinių paslapčių, teisės į reputaciją, nuosavybės teisių elektroninėje erdvėje apsaugą, įgyvendinant kibernetinio saugumo talentų projektą ir skatinant kibernetinio saugumo mokslo įstaigų plėtrą (numatyta įsteigti kibernetinio saugumo akademijas ir inovacijų parkus).

7. *Didinti kibernetinės erdvės gynybos galimybes.* Užduoties įgyvendinimas apibrėžtas lakoniškai: „sukurti kibernetinio saugumo apsaugos pajėgas, proporcingas šalies tarptautinei padėčiai“.

8. *Stiprinti tarptautinį bendradarbiavimą.* Įgyvendinant šią užduotį strategijoje numatytas pasaulinės interneto valdymo reformos skatinimas; Jungtinių Tautų Organizacijos veiklos, susijusios su kibernetiniu saugumu, rėmimas; paramos besivystančioms šalims ir atsilikusiems regionams teikimas; skaitmeninės atskirties mažinimas.

Apibendrinant strategijoje numatytas užduotis pastebėtina, kad Kinija siekia stiprinti ypatingos svarbos informacijos infrastruktūros apsaugą, sukurti sklandžiai funkcionuojančią kibernetinio saugumo valdymo sistemą, taip pat pripažįsta bendradarbiavimo nacionaliniu ir tarptautiniu mastu svarbą. Taip pat akcentuoja paramą mokslo plėtrai kibernetinio saugumo srityje, visuomenės švietimo svarbai. Įdomu ir tai, kad strategijoje piliečiai skatinami skleisti tik pozityvią informaciją apie kinų kultūrą.

Strategijoje išskiriamos šios kibernetinio saugumo **grėsmės**: terorizmas ir šnipinėjamas elektroninėje erdvėje, internetinis sukčiavimas, vagystės, prekyba narkotinėmis medžiagomis ir ginklais, piliečių asmeninės informacijos pažeidimai, nepadorumo ir sekso skatinimas, intelektinės nuosavybės teisių pažeidimai.

Analizuojant dokumento turinį svarbu paminėti ir tai, kad kibernetinio saugumo strategijos priėmimu ir įgyvendinimu taip pat siekiama stiprinti Kinijos komunistų partijos autoritetą, vidinį šalies stabilumą, užkirsti kelią socialiniams ir politiniams neramumams, skatinti ekonomikos augimą.

Bijoma, kad neribotas ir nekontroliuojamas naudojimasis informacinėmis technologijomis gali daryti neigiamą įtaką komunistų partijos ir visos valstybės stabilumui.

Autoriaus manymu vienas iš esminių Kinijos kibernetinio saugumo strategijos trūkumų yra tas, kad joje nenustatyta aiškus joje suformuluotų priemonių įgyvendinimo planas, nenurodytos institucijos, atsakingos už numatytų strateginių užduočių vykdymą. Be abejo, neatmetama galimybė, kad priemonių įgyvendinimo planas egzistuoja, tačiau jo tekstas nepaskelbtas ir nesusietas su viešai prieinamu strategijos vertimu į anglų kalbą.

Vadovaujantis mokslinėje literatūroje[61] pateikta informacija, Kinijoje kibernetinio saugumo politiką įgyvendina šie subjektai: Kinijos komunistų partijos nuolatinis komitetas, Centrinė karinė komisija, Valstybės taryba, Mokslo, technologijų ir krašto apsaugos pramonės komisija, ministerijos (Pramonės ir informacinių technologijų, Viešojo saugumo, Valstybės saugumo), Mokslo, technologijų ir krašto apsaugos pramonės administracija, Valstybės paslapčių biuras, Valstybės šifravimo biuras, Nacionalinio saugumo komisija, atskiri Liaudies išsilaisvinimo armijos padalinai, taip pat mokslo ir inovacijų institucijos (Karo akademija, Užsienio kalbų universitetas, Informatikos inžinerijos universitetas, kitos mokslo akademijos ir mokslinių tyrimų centrai). Konkrečios šių subjektų funkcijos ir įgaliojimai įgyvendinant kibernetinio saugumo strategiją nenurodyti.

Apibendrinant Kinijos kibernetinio saugumo strategiją galima daryti pagrįstą išvadą, kad dokumentas nacionalizuotas ir gali būti siejamas su „Chinese Dream“[62] sąvoka, kurios autorius yra Kinijos komunistų partijos generalinis sekretorius Xi Jinping. Strategijoje teigiama, kad kibernetinės grėsmės kenkia ir šalies politiniam saugumui, informacinės technologijos naudojamos siekiant kištis į kitų valstybių vidaus reikalus, pulti jų politines sistemas, kurstyti socialinius neramumus, o plataus masto kibernetinis stebėjimas, šnipinėjimas ir kitokia neteisėta veikla kibernetinėje erdvėje daro žalą tiek valstybės politiniam saugumui, tiek atskirų vartotojų informacijos saugumui.

Baigiant Kinijos kibernetinio saugumo strategijos analizę, būtina paminėti ir tai, kad Kinija užima pirmąją vietą daugiausiai programišių turinčių pasaulio valstybių sąraše[63]. Elektroninio šnipinėjimo veikla itin išplėtota[64]. Vienas iš naujausių kibernetinių atakų, dėl kurios kaltinami Kinijos programišiai – įsilaužimas į Microsoft elektroninio pašto serverio programinę įrangą 2021 m. vasario

[61] Jimmy Goodrich, “Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy,” in China and Cybersecurity: Political, Economic, and Strategic Dimensions, Report from workshops held at the University of California, San Diego (April 2012), 5-6. Prieiga internetu: http://igcc.ucsd.edu/assets/001/503568.pdf

[62] Terminas, apibūdinantis asmeninius ir valstybinius idealus Kinijoje. Jo esmė: jauni žmonės turi išdrįsti svajoti ir atkakliai dirbti, kad tas svajones išpildytų ir prisidėtų prie tautos atgaivinimo. Šaltinis internetu: https://en.wikipedia.org/wiki/Chinese_Dream

[63] Kitos į “septynetuką” patekusios valstybės mažėjimo tvarka: Jungtinės Amerikos Valstijos, Turkija, Rusija, Taivanas, Brazilija ir Rumunija. Šaltinis internetu: https://abcnews.go.com/Technology/slideshow/top-hacking-countries-19844818/image-19845656

[64] Daniel R. Coats, „World wide threat assessment of the US intelligence community“, 2019 m. P. 5.

mėn.[65]. Be abejo, tai tuo pačiu rodo ir aukštą žinių lygį kibernetinio saugumo srityje, taip pat gebėjimus prognozuoti kibernetinius išpuolius ir užkirsti jiems kelią.

Pietų Korėjos kibernetinio saugumo strategija parengta ir publikuota 2019 m. balandį, tačiau tai nereiškia, kad anksčiau šalis neskyrė dėmesio kibernetinio saugumo problemoms ir nebuvo parengusi kibernetinio saugumo aspektus reglamentuojančių teisės aktų. Iki kibernetinio saugumo strategijos parengimo ir paskelbimo, Pietų Korėjoje veikė Tinklų strategija, kurios reguliavimo sritis apėmė ir kibernetinio saugumo klausimus.

2019 m. kibernetinio saugumo strategija[66] aiškiai struktūriškai išdėstyta (įžanginis žodis, trumpa esamos situacijos apžvalga, strategijos vizija, tikslai ir užduotys), apimtis – 27 puslapiai. Strategijoje nurodoma, kad ji parengta atsižvelgiant į valstybės Nacionalinio saugumo strategiją. Be to, papildomai su šia kibernetinio saugumo strategija parengtas Nacionalinį kibernetinio saugumo planas ir plane numatytų priemonių įgyvendinimo planas.

Strategijos **vizija**: sukurti laisvą ir saugią elektroninę erdvę, užtikrinti nacionalinį saugumą, skatinti ekonominę gerovę ir prisidėti prie tarptautinės taikos. Pažymėtina, kad Pietų Korėja strategijoje pristato save kaip lyderiaujančią informacinių technologijų srityje valstybę ir kviečia visus piliečius prisijungti prie kibernetinio saugumo iniciatyvų, kad šalis ir toliau išliktų lyderė. Tai nestebina, nes ši valstybė laimėjo lenktynes, kas pirmasis pasiūlys 5G ryšį visos šalies naudotojams. Vis tik nereikia pamiršti, kad 5G technologijų srityje dominuoja Kinijos bendrovės. Bendrovė „Huawei“ yra užregistravusi 1,529 tūkst. Patentų, susijusių su 5G. Kartu su Kinijos gamintojais „ZTE“, „Oppo“ ir bendrove „China Academy of Telecommunications Technology“ Kinijai priklauso 3,4 tūkst. su 5G susijusių patentų. Tuo tarpu Pietų Korėja pagal su 5G susijusių patentų skaičių užima antrą vietą, jos bendrovėms priklauso 2,051 tūkst. patentų[67].

Kibernetinio saugumo strategijos **principai**:

1) balansas tarp kibernetinio saugumo ir žmogaus teisių užtikrinimo;

2) kibernetinio saugumo veiklos vykdymas laikantis įstatymų;

3) sistema, skatinanti dalyvauti ir bendradarbiauti. Kibernetinio saugumo užtikrinimas traktuojamas ne kaip išskirtinai valstybės rūpestis, į užtikrinimo priemonių įgyvendinimą įtraukiami verslo subjektai ir gyventojai.

Strategijoje suformuluoti šie tikslai:

[65] Chinese Hackers Blamed for Massive Microsoft Server Hack. The Diplomat, March 10, 2021. Šaltinis internetu: https://thediplomat.com/2021/03/chinese-hackers-blamed-for-massive-microsoft-server-hack/

[66] Prieiga internetu: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf

[67] Pietų Korėjoje pradės veikti pirmieji pasaulyje nacionaliniai 5G tinklai, 2019. DELFI, Mokslas Technologijos. Prieiga per internetą: <https://www.delfi.lt/mokslas/technologijos/pietu-korejoje-prades-veikti-pirmieji-pasaulyje-nacionaliniai-5g-tinklai.d?id=80814131>.

1. *Stabilaus valstybės darbo užtikrinimas.* Siekiama sustiprinti pagrindinės valstybės infrastruktūros saugumą ir atsparumą kibernetinėms grėsmėms.

2. *Reagavimas į kibernetines atakas.* Šiuo tikslu siekiama sustiprinti saugumo pajėgumus, kad būtų galima išvengti kibernetinių grėsmių arba jas greitai aptikti, nukenksminti ir nedelsiant sureaguoti į bet kokį incidentą kibernetinėje erdvėje.

3. *Tvirtų kibernetinio saugumo pagrindų sukūrimas,* t. y. siekiama sukurti ir palaikyti teisingą ir autonomišką ekosistemą, kurioje konkurencingai veiktų kibernetinio saugumo technologijos, žmogiškieji ištekliai, į ekosistemą būtų įtrauktos visos pramonės šakos.

Apibendrinant galima teigti, kad nurodyti tikslai yra orientuoti į saugumo kibernetinėje erdvėje užtikrinimą, saugumo pajėgumų didinimą ir rizikų identifikavimą bei kontrolę.

Atkreiptinas dėmesys, kad Pietų Korėja kibernetinio saugumo strategijoje ne tik nurodė konkrečius siektinus tikslus, bet ir akcentavo iššūkius, verčiančius skirti didesnį dėmesį kibernetiniam saugumui: padidėjęs elektroninės erdvės pažeidžiamumas, kibernetinių grėsmių sunkumas (atakas vykdo ne vien pavieniai asmenys ar jų grupės, bet ir valdžios atstovų remiamos teroristinės organizacijos, incidentai tampa geriau organizuoti, plečiasi jų poveikio laukas), vyksta aktyvesnė kibernetinio saugumo konkurencija tarp valstybių, ženkliai didėja nusikalstamomis veikomis kibernetinėje erdvėje daroma žala visuomenei.

Strateginės užduotys šešios, kiekviena jų detalizuojama ir nurodoma, kokie konkretūs veiksmai ir sprendimai turi būti priimti, siekiant užduočių įgyvendinimo. Trumpai aptarsiu kiekvieną strateginę užduotį.

1. *Didinti nacionalinės kritinės infrastruktūros objektų saugumą.* Užduotis įgyvendinama stiprinant nacionalinių informacijos ir ryšių tinklų apsaugą (nemažai dėmesio skiriama kriptografijai ir kitoms konfidencialios informacijos saugumą užtikrinančioms priemonėms); gerinant kritinių infrastruktūrų objektų kibernetinio saugumo aplinką, diegiant saugumo vertinimo standartus ir steigiant atskirus padalinius, atsakingus už jų įgyvendinimą; kuriant naujos kartos kibernetinio saugumo aplinką, kurioje kiekvienas visuomenės narys galėtų patogiai ir saugiai naudotis informacinių technologijų paslaugomis ir dirbtiniu intelektu pagrįsta aplinka.

2. *Gerinti reagavimo į kibernetines atakas pajėgumus.* Tai vykdoma atgrasant kibernetines atakas, nedelsiant reaguojant į jas ir nustatant atakas vykdžiusius subjektus, taip pat sukuriant visapusiškas ir aktyvias atsakomąsias priemones, įskaitant įspėjimus apie potencialias atakas, dalijimąsi informacija, mokslinių tyrimų atlikimo skatinimą ir rėmimą.

3. S*ukurti pasitikėjimu ir bendradarbiavimu pagrįstą valdymo sistemą.* Siekiama, kad kibernetinio saugumo užtikrinimo srityje bendradarbiautų viešasis, privatus ir karinis sektoriai, informacija būtų dalijamasi visos šalies mastu (numatoma įdiegti specialią dalijimosi informacija sistemą), taip pat nurodomas poreikis tobulinti šalies kibernetinio saugumo teisinę bazę.

4. *Sukurti pamatus kibernetinio saugumo pramonės plėtrai*. Įgyvendinant šią užduotį numatoma didinti investicijas kibernetiniam saugumui užtikrinti (tiek iš valstybės biudžeto, tiek per mokesčius, tiek įtraukiant verslo subjektus), plėsti valstybėje jau veikiančios informacinės sistemos „Vieši pranešimai apie informacijos saugumą“ pajėgumus, skatinti informacinių technologijų ir saugumo srityse dirbančių specialistų konkurenciją, įgyvendinti sąžiningos konkurencijos principą kibernetinio saugumo srityje.

5. *Puoselėti kibernetinio saugumo kultūrą.* Įgyvendinant šią užduotį ypač pabrėžiama būtinybė išlaikyti balansą tarp kibernetinio saugumo ir pagrindinių žmogaus teisių. Taip pat akcentuojamas specializuotų mokymų atskiroms visuomenės grupėms (studentams, verslui, valstybės pareigūnams, kariškiams) svarba.

6. *Vadovauti tarptautiniam bendradarbiavimui kibernetinio saugumo srityje.* Pažymėtina, kad strategijoje kalbama būtent apie vadovavimą (ne dalyvavimą, prisidėjimą, užtikrinimą ar pan.), kas dar kartą pabrėžia tai, kad Pietų Korėja laiko save lydere kibernetinio saugumo politikos formavimo srityje ir neketina užleisti šios pozicijos. Detalizuojant užduotį nurodoma, kad ją įgyvendinant bus gerinamos dvišalio ir daugiašalio bendradarbiavimo sistemos, užtikrinama lyderystė tarptautiniame bendradarbiavime (iniciatyva dalinantis gerąja patirtimi ir praktika, aktyvus įsitraukimas į tarptautines diskusijas, pagalba besivystančioms šalims).

Pietų Korėjos 2019 m. kibernetinio saugumo strategijoje nurodytos kibernetinio saugumo **grėsmės** originalumu nepasižymi. Nurodytos šios grėsmės: pavieniai nusikaltėlių ir nusikalstamų grupuočių veiksmai kibernetinėje erdvėje, kibernetinis terorizmas, konfidencialios informacijos ir pinigų vagystės, socialiniai neramumai.

Pietų Korėjos, kaip ir Kinijos, kibernetinio saugumo strategijos **trūkumas** yra tas, kad joje trūksta informacijos apie numatytas strategines užduotis įgyvendinančius subjektus, jų funkcijas, atsakomybę, įgaliojimų ribas. Strategijoje suformuluotų užduočių įgyvendinimo planui skirtas tik vienas – paskutinis – puslapis, kuriame nurodoma, kad valstybė prisiima atsakomybę už strategijos įgyvendinimą ir skatina bendradarbiavimą su piliečiais, įmonėmis ir tarptautine bendruomene. Visos ministerijos ir agentūros privalo siekti strategijoje numatytų tikslų, o kontrolės ir priežiūros funkcija pavedama Nacionaliniam saugumo biurui.

Strategijoje taip pat nurodoma, kad kibernetinio saugumo politika Pietų Korėjoje grindžiama visuomenės pasitikėjimu, todėl valstybė yra visiškai atvira bendradarbiavimui tiek su fiziniais asmenimis, tiek su verslo subjektais. Tai pažangus požiūris, tačiau jo įgyvendinimas praktikoje priklauso nuo šalies tradicijų, visuomenės išsivystymo ir kultūros lygmens, kitų aspektų, kurių valstybė negali sukontroliuoti.

Apibendrinant Pietų Korėjos kibernetinio saugumo strategiją galima teigti, kad tai puikiai struktūrizuotas ir pakankamai lengvai suprantamas, su aiškiai suformuluotais tikslais, konkrečiomis ir

realiai pasiekiamomis jų įgyvendinimo priemonėmis, tačiau nepasižymintis išskirtiniu originalumu dokumentas.

Taip pat norėtųsi pažymėti, kad Pietų Korėjos didžiavimasis pasiekimais kibernetinio saugumo srityje nėra nepagrįstas. Kasmet 194 valstybes vienijanti Jungtinių Tautų Tarptautinė telekomunikacijų sąjunga įvertina valstybių pastangas adaptuoti nacionalinę teisinę bazę, įgyvendinti techninius-organizacinius reikalavimus, vystyti pajėgumus ir bendradarbiavimą kibernetinio saugumo sektoriuje. Pagal Globalų kibernetinio saugumo indeksą Pietų Korėja regioniniame reitinge užėmė 5, o globaliajame – 15 vietą[68].

Australija šiuo metu įgyvendina jau trečiąja kibernetinio saugumo strategiją. 2009 m. strategija buvo aptarta 2.1 šio darbo poskyryje, ją pakeitė 2016 m. strategija[69], iškėlusi penkis iki 2020 m. įskaitytinai įgyvendintinus tikslus:

1. *Vidinis bendradarbiavimas kibernetinio saugumo srityje* (omenyje turima glaudi partnerystė su privačiu sektoriumi). Bendradarbiavimas vykdomas per kasmetinius susitikimus, į kuriuos taip pat numatoma kviesti akademinės bendruomenės narius ir kartu aptarti visas iškilusias problemas, galimus jų sprendimo būdus. Bendradarbiavimas stiprinamas ir per plečiamus Australijos Kibernetinio saugumo centro įgaliojimus.

2. *Stipri kibernetinės erdvės apsauga.* Didžiuosiuose miestuose steigiami dalijimosi informacija apie kibernetines grėsmes centrai (juose telkiamas viešojo ir privataus sektorių personalas, sprendimai priimami bendru sutarimu), taip pat įkurta elektroninė informacijos apie kibernetines grėsmes platforma. Numatomas ženklus specialistų (informacinių technologijų, saugumo, taip pat tiriančių elektroninius nusikaltimus) skaičiaus didinimas.

3. *Pasaulinė įtaka ir atsakomybė.* Australijos ambicijos ir siekis būti lydere formuojant tarptautinę kibernetinio saugumo politiką nei kiek nenusileidžia Pietų Korėjos siekiams. Numatoma paskirti Kibernetinių reikalų ambasadorių, kurio pagrindinė funkcija būtų identifikuoti praktines tarptautinio bendradarbiavimo galimybes ir užtikrinti, kad Australija aktyviai jas išnaudotų. Numatoma ir parama Indijos ir Ramiojo vandenyno regiono šalims plečiant gebėjimus kibernetinio saugumo srityje.

4. *Inovacijos ir plėtra.* Ir toliau skatinamos inovacijos, finansuojami moksliniai tyrimai, teikiama parama bendrovėms, galinčioms pasiūlyti naujų inovatyvių sprendimų kibernetinio saugumo srityje. Planuojama įkurti Kibernetinio saugumo plėtros centrą, jungianti viešąsias ir privačias įmones, mokslininkus ir ieškantį galimybių verslo plėtrai, startuoliams, užsienio investicijoms kibernetinio saugumo srityje. Be to, steigiamos specialios stipendijos šioje srityje dirbantiems doktorantams.

---

[68] Jungtinių Tautų Tarptautinė telekomunikacijų sąjunga, *Globalus kibernetinio saugumo indeksas, 2018.* Prieiga per internetą: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[69] Prieiga internetu: https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf

5. *Kiber-išmani valstybė.* Tikslas ypač orientuotas į švietimą ir kvalifikuotų darbuotojų skaičiaus didinimą. Universitetuose steigiami Kibernetinio saugumo kompetencijos centrai, taip pat siekiama, kad tiek pradinių klasių moksleiviai, tiek abiturientai būtų išklausę atitinkamas jų amžių atitinkančias programas, o įvairūs mokymai ir seminarai būtų prieinami pačių įvairiausių sektorių darbuotojams.

Tikslams įgyvendinti 2016 m. strategijoje numatytas priemonių planas su vykdytojais bei įvykdymo rezultatų vertinimo kriterijais.

Pažymėtina, kad jau iš 2016 m. strategijos aiškiai matyti Australijos pažanga, įgyvendinant kibernetinio saugumo priemones. Dėl šios priežasties strategijoje nėra būtinybės kelti tokių tikslų kaip „siekti“, „stengtis“, „pasiekti“, „ieškoti būdų“. Daug kas jau sėkmingai pasiekta, būdai rasti, priemonės įgyvendintos, atsakingos institucijos įsteigtos ir sėkmingai veikiančios, todėl belieka tik „gerinti“, „tobulinti“, „plėsti“. Be abejo, tai neįmanoma be investicijų (į šioje strategijoje numatytų priemonių įgyvendinimą investuota 230 mln. Australijos dolerių) ir kiekvieno bendruomenės nario įsitraukimo. Nereikėtų pamiršti ir to, kad Australija itin „kompiuterizuota“ tauta, t. y.: 2016 m. 2 iš 3 australų turėjo paskyras socialinėse platformose, tokiose kaip „Facebook“ ar „Instagram“, 84 proc. smulkiojo ir vidutinio verslo atstovų teikė paslaugas on-line; australai įprastai internete (ne darbo reikalais) praleidžia 24 val. per savaitę[70].

Šiuo metu Australija įgyvendina 2020 m. rugpjūčio 6 d. priimtą kibernetinio saugumo strategiją[71]. Savo turiniu, informacijos pateikimu, jos iliustravimu citatomis, pavyzdžiais strategija primena Jungtinės Karalystės 2016 m. kibernetinio saugumo strategiją, todėl dokumentas taip pat vertintinas kaip gerosios praktikos pavyzdys.

Sektina tai, kad neapsieinama be pasiektų rezultatų įvertinimo ir nurodoma, kad labiausiai didžiuojamasi šiomis įgyvendintomis kibernetinio saugumo priemonėmis: Kibernetinio saugumo centro atidarymu ir veiklos plėtra, Jungtinių kibernetinio saugumo centrų įsteigimu, ženkliai pagerėjusiu gyventojų informuotumu apie saugų elgesį elektroninėje erdvėje (Vyriausybė strategijos įgyvendinimo metu suteikė 1400 asmeninių (face-to-face) konsultacijų gyventojams), 24/7 Visuotinio stebėjimo platformos[72] įdiegimas, Kibernetinių reikalų ambasadoriaus paskyrimas, Jungtinio kibernetinio saugumo tyrimų centro įsteigimas.

Vizija: dar saugesnė kibernetinė aplinka australams, verslui ir būtinųjų paslaugų teikimui. Pabrėžiama, kad vizijos, kaip ir ankstesnėse strategijose, bus siekiama jungtinėmis valstybės, privataus sektoriaus ir kiekvieno gyventojo pastangomis.

---

[70] Šaltinis internete: https://www.genroe.com/blog/social-media-statistics-australia/13492

[71] Prieiga internetu: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

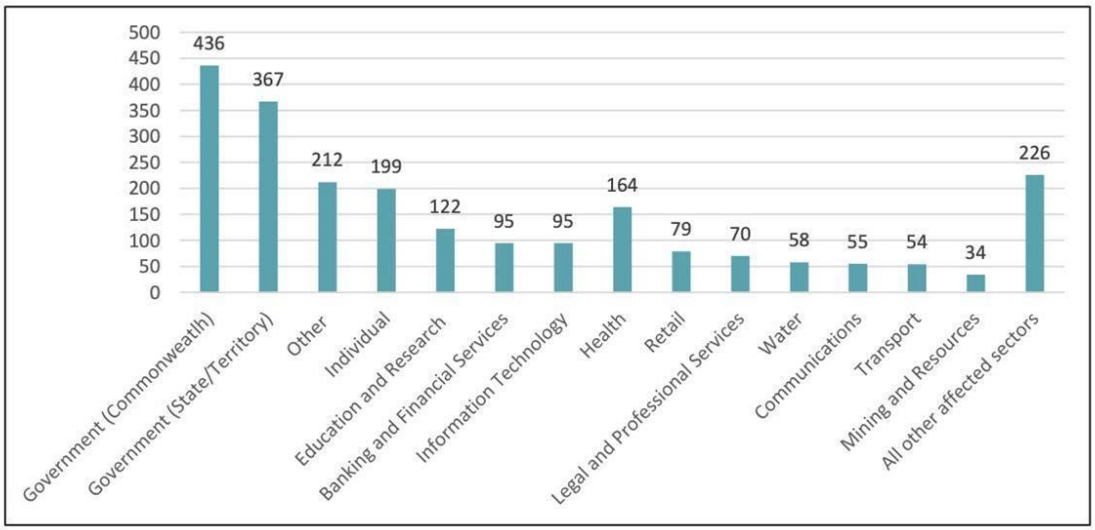
[72] Nuotoliniu būdu teikiamos konsultacijos apie saugų elgesį internete, ypač aktualios vyresnio amžiaus žmonėms ir vaikams. Plačiau: https://blog.paloaltonetworks.com/2020/08/policy-australia-2020-cyber-security-strategy/

Iš valstybės tikimasi saugios kibernetinės aplinkos garantavimo verslui, gyventojams bei būtinųjų paslaugų teikimui. Verslo įmonės privalės (ir privalėjo pagal ankstesnes strategijas) užtikrinti parduodamų produktų ir teikiamų paslaugų saugumą, apsaugoti klientus nuo kibernetinių grėsmių verslo veikimo sferoje. Gyventojai privalo prisiimti atsakomybę už saugų elgesį elektroninėje erdvėje ir saugumo standartų laikymąsi.

Nepaisant sėkmingai įgyvendinamų kibernetinio saugumo strategijose numatytų priemonių, kibernetinių incidentų skaičius išlieka didelis. Per metus (nuo 2019 m. liepos 1 d. iki 2020 m. birželio 30 d. Australija patyrė 2266 kibernetinius incidentus, kurių daugiausiai (436 ir 367) buvo nukreipti į aukščiausiąsias ir vietos valdžios institucijas (Pavyzdys Nr. 2). Be to kibernetinių incidentų pobūdį įtakoja ir COVID-19 pandemija. Australijos Kibernetinio saugumo centro duomenimis[73], nuo 2020 m. kovo 10 d. iki 2020 m. kovo 26 d. (vos per dvi savaites) gauti 45 pranešimai apie kibernetines atakas, susijusias su kenkėjiškos programinės įrangos platinimu ir bandymu pagrobti vartotojų asmens duomenis.

Pavyzdys Nr. 5

Figure 3: Cyber security incidents, by affected sector (1 July 2019 to 30 June 2020)



Šaltinis: ACSC countered 2266 cyber security incidents last year. IT news, by Justin Hendry, September 4, 2020. https://www.itnews.com.au/news/acsc-countered-2266-cyber-security-incidents-last-year-552858.

Strategijoje išskiriamos šios kibernetinius incidentus sukeliančių asmenų grupės: 1) *užsienio valstybių ir valstybės remiamos grupuotės,* siekiančios prieiti prie svarbios ekonominės, finansinės, teisinės, politinės, gynybos ir saugumo informacijos. Jų veiksmai vertintini kaip itin pavojingi ir potencialiai galintys sukelti didžiausią žalą; 2) *finansinės naudos siekiantys nusikaltėliai* (nerimą kelią

[73] Plačiau: https://www.cyber.gov.au/acsc/view-all-content/advisories/threat-update-covid-19-malicious-cyber-activity-20-april-2020

augantys prekybos vogtomis tapatybėmis ir vaikų išnaudojimo atvejai); 3) *dėmesio siekiantys nusikaltėliai* (jų esminis tikslas – pademonstruoti gebėjimus. Jiems neretai trūksta techninio pasirengimo, tačiau sukeliamos pasekmės gali būti itin žalingos); 4) *teroristai ir ekstremistai* (šiuo metu Australijoje jų išpuoliai reti).

Strategijoje pripažįstama, kad nepaisant įdiegtų techninių apsaugos priemonių, įsteigtų ir sėkmingai veikiančių kibernetinio saugumo institucijų, gerėjančio gyventojų informuotumo apie saugų elgesį elektroninėje erdvėje, kibernetinių incidentų skaičius išlieka didelis ir jo mažėjimų tendencijų prognozuoti negalima. Kibernetinio incidento pasekmes patyrė kas trečias pilnametis australas. Australijos kibernetinio saugumo centras pranešimą apie įvykusį incidentą ar elektroninį nusikaltimą gauna beveik kas 10 minučių. Tai rodo, kad reikia ieškoti naujų apsaugos būdų ir priemonių bei telkti pastangas juos įgyvendinant.

2020 m. kibernetinio saugumo strategijos įgyvendinimo priemonių plane numatytos priemonės skirstomos į jas įgyvendinti turinčias subjektų grupes, t. y. valstybę, verslo subjektus ir gyventojus. Priemones numatoma įgyvendinti iki 2030 m., jų įgyvendinimui finansuoti numatyta skirti 1,67 bln. Australijos dolerių, kiekvienos plane numatytos priemonės įgyvendinimui skirta konkreti suma.

Aptarsiu įdomesnes ir potencialiai galinčias būti pritaikytas Lietuvos kibernetinio saugumo strategijoje priemones.

1. Priemonės, už kurių įgyvendinimą atsakinga **valstybė:** *kritinės infrastruktūros objektų apsaugos stiprinimas* (numatomi reagavimo į incidentą laiko ir efektyvumo faktoriai); *veiksmų tamsiajame internete (Dark Web*[74]*) teisinis reglamentavimas*, pasitelkiant į pagalbą teisėsaugos institucijas; *keitimosi informacija apie kibernetinius incidentus tobulinimas* (įtraukiami privataus sektoriaus subjektai, siekiama abipusio keitimosi informacija realiu laiku); *teisiškai reglamentuoti privataus sektoriaus subjektų atsakomybę* už kibernetinio saugumo priemonių įgyvendinimą; *neatsilikti nuo techninio progreso* (operatyviai nustatomi technologijų pažeidžiamumai ir, pasitelkus mokslininkus, imamasi veiksmų jiems spręsti).

2. Priemonės, už kurių įgyvendinimą atsakingi **privataus sektoriaus subjektai**: *siūlymų kritinės infrastruktūros saugumo būklei gerinti teikimas* (bendradarbiavimas su privačiu sektoriumi šioje srityje buvo įtrauktas ir į 2016 m. strategijos priemonių planą); *užtikrinti kibernetinio saugumo priemonių įgyvendinimą smulkiosiose įmonėse; plėtoti daiktų internetą*[75]*; tobulinti darbuotojų kvalifikacijas ir žinias kibernetinio saugumo srityje.*

[74] Tamsusis internetas – nekontroliuojama interneto dalis, egzistuojanti tamsiajame tinkle, kuriam pasiekti reikia specializuotos programinės įrangos, konfigūracijos ar autorizacijos. Paieškos sistemos tinklo neindeksuoja ir jame galima rasti tokios informacijos kaip vaikų pornografija, prekyba organais ir pan. Šaltinis internetu: https://lt.wikipedia.org/wiki/Tamsusis_internetas

[75] 2016 m. Australijos kibernetinio saugumo strategijoje buvo prognozuojama, kad 2019 m. vidutinis šeimos ūkis naudosis 24 interneto ryšiu susietais įtaisais.

3. Priemonės, už kurių įgyvendinimą atsakinga **visuomenė:** *vadovautis naujausiomis rekomendacijomis apie saugų elgesį internete; susidūrus su kibernetiniu incidentu, nedelsiant kreiptis pagalbos ar konsultacijų* (ypač skatinama naudotis 24/7 Visuotinio stebėjimo platformos galimybėmis); *naudotis tik saugumo standartus atitinkančiomis informacinėmis technologijomis; pranešti apie žinomą elektroninį nusikaltimą.*

Dalis išvardytų priemonių formuluojamos kaip rekomendacijos, vis tik jų įtraukimas į kibernetinio saugumo strategijos priemonių planą ženkliai prisideda prie kiekvieno visuomenės nario sąmoningumo formavimo.

Apibendrinimas:

1. Australija vertintina kaip viena labiausiai pažengusių kibernetinio saugumo srityje valstybių. Šalies kibernetinio saugumo strategijos galėtų būti sektinu pavyzdžiu daugeliui valstybių. Strategijos vizualiai patraukliai pateiktos, jose gausu pavyzdžių, statistikos, aiškus numatomų įgyvendinti tikslų tęstinumas;

2. Bendradarbiavimas su privataus sektoriaus subjektais itin pažangus. Privataus sektoriaus subjektai laikomi lygiaverčiais partneriais, keitimasis informacija, patirtimi vyksta dvipusiai, kylančios problemos sprendžiamos kartu;

3. Kaip geroji praktika vertintinos priemonės, leidžiančios operatyviai gauti pagalbą ir konsultacijas, susidūrus su kibernetiniu incidentu (24/7 Visuotinio stebėjimo platforma);

4. Itin daug pastangų dedama siekiant įtraukti visuomenę į kibernetinio saugumo priemonių vykdymą. Puikiai suvokiama, kad net ir pačios geriausios techninės apsaugos priemonės negali eliminuoti žmogiškosios klaidos, todėl skatinama asmeninė atsakomybė už saugaus elgesio internete standartų laikymąsi.

2.7 Italijos, Ispanijos ir Portugalijos kibernetinio saugumo strategijų panašumai ir skirtumai

Italija, Portugalija ir Ispanija kibernetinio saugumo įgyvendinimo procese susiduria su panašiais iššūkiais, tačiau savo nacionalinėse kibernetinio saugumo strategijose numato skirtingas priemones jiems spręsti.

2013 m. sausio 24 d. Italijos Ministro Pirmininko dekretu patvirtintos Kibernetinės erdvės apsaugos ir informacinių technologijų saugumo gairės, kuriose skatinama parengti prioritetinių priemonių, skirtų tiek viešajam, tik privačiam sektoriui, įgyvendinimo planą.

Italijos Kibernetinio saugumo veiksmų planas patvirtintas daugiau nei po ketverių metu, tik 2017 m. kovo mėn.[76], įgyvendinant 2017 m. vasario 17 d. Kibernetinio saugumo direktyvą. Ši direktyva priimta, siekiant įgyvendinti TIS direktyvos nuostatų reikalavimus ir tai labai aiškiai matyti, analizuojant Kibernetinio saugumo veiksmų planą.

Delsimas parengti planą, numatantį kibernetinio saugumo įgyvendinimo priemones, sunkiai paaiškinamas, nes Italija nėra priskirtina valstybėms, galinčioms pasigirti nedideliu kibernetinių incidentų skaičiumi. Vien *phishing*[77] duomenų vagysčių skaičius nuo 400 2015 m. išaugo iki 3000 2019 m.[78]. Nuo kibernetinių atakų 2015–2016 m. nukentėjo 45,2 proc. įmonių, o įmonių skiriamų lėšų kibernetinių incidentų prevencijai suma buvo itin kukli – apie 4530 Eur per metus[79].

Išsikelti **tikslai** originalumu nepasižymi. Siekiama:

1) didinti visų suinteresuotų subjektų techninę ir analitinę patirtį, sprendžiant kibernetinio saugumo problemas;

2) stiprinti kritinės infrastruktūros objektų apsaugą;

3) skatinti viešojo ir privataus sektoriaus bendradarbiavimą;

4) skatinti ir vystyti kibernetinio saugumo kultūrą;

5) stiprinti pajėgumus kovojant su elektroniniais nusikaltimais, piktavališka ir neteisėta veikla kibernetinėje erdvėje;

6) stiprinti tarptautinį bendradarbiavimą.

Paanalizuosiu plane numatytas kibernetinio saugumo priemones.

1. *Priemonės, skirtos kibernetinio saugumo srities teisiniam reglamentavimui tobulinti ir elektroninės erdvės atsparumui bei saugumui stiprinti.* Autoriaus nuomone, plane pažodžiui atkartojamos TIS direktyvos nuostatos o veiksmai, kurie turėtų būti atlikti dar prieš plano parengimą ir patvirtinimą, įvardijami kaip atskiros priemonės, t. y. kibernetinės erdvės pažeidžiamumų ir jai kylančių grėsmių įvertinimas, kibernetinės gynybos pajėgumų įvertinimas, kibernetinių incidentų apskaita. Teigiamai vertintinos tokios priemonės kaip bendradarbiavimas su universitetais ir mokslinių tyrimų centrais, kuriant ir diegiant technines saugumo priemones, viešojo ir privataus sektorių keitimasis informacija apie incidentus ir jų prevencijos priemones, kibernetinės gynybos institucijų pajėgumų stiprinimas (nors nenurodžius, kaip tai bus daroma (investicijomis, personalo skaičiaus didinimu, atitinkamų funkcijų suteikimu ar esamų funkcijų išplėtimu, naujų padalinių steigimu), ši priemonė gali likti deklaratyvi ir realiai neįgyvendinta).

---

[76] Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Italy.

[77] Phishing duomenų vagystė – tai tokia sukčiavimo forma, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar suklastotais interneto tinklalapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius ir kitus konfidencialius duomenis. Šaltinis internetu: https://www.nksc.lt/rekomendacijos/phishing.html

[78] Plačiau: https://www.statista.com/topics/4102/cybersecurity-in-italy/

[79] The future of Cybersecurity in Italy: Strategic focus areas. Roberto Baldoni, Laboratorio Nazionale di Cybersecurity, 2018. P. 8.

2. *Priemonės, skirtos viešojo ir privataus sektorių bendradarbiavimui stiprinti.* Priemonių plane nurodoma, kad esminė glaudaus bendradarbiavimo būtinumo priežastis yra ta, kad Italijoje kritinės reikšmės infrastruktūros objektus valdo privačios organizacijos. Bendradarbiavimo stiprinimui numatytos tokios priemonės kaip reagavimo į kibernetines grėsmes operatyvumo skatinimas, paramos teikimas (neaišku, ar finansinės, ar informacinės, ar kokios nors kitos), vertinimo kriterijų ypatingos svarbos infrastruktūros objektų informacinių sistemų pažeidžiamumui nustatymas, privataus sektoriaus subjektų įtraukimas į renginius ir pratybas kibernetinio saugumo klausimais.

Pažymėtina, kad ši priemonių grupė dėl iniciatyvos skatinti ir stiprinti bendradarbiavimą sulaukė kritikos ir pačioje Italijoje[80].

3. *Priemonės, skirtos kibernetinio saugumo kultūrai suformuoti, švietimui ir kvalifikacijos šioje srityje tobulinimui.* Pagirtina tai, kad į mokymų kibernetinio saugumo srityje procesą ketinama įtraukti ne tik saugumo ir informacinių technologijų sričių darbuotojus (jiems numatomi specializuoti kvalifikacijos tobulinimo kursai), bet ir viešojo bei privataus sektorių atstovus, gyventojus. Kitos priemonės – domėjimasis naujovėmis kibernetinio saugumo užtikrinimo srityje bei įsitraukimas į Europos Sąjungos ir NATO iniciatyvas – nėra pagrindžiamos konkrečiais veiksmais.

4. *Priemonės, skirtos tarptautiniam bendradarbiavimui stiprinti.* Numatoma stiprinti tiek dvišalį, tiek daugiašalį bendradarbiavimą, aktyviai įsitraukti į tarptautinius forumus, dalyvauti tarptautinėse kibernetinio saugumo pratybose (į dalyvavimą įtraukiami privataus sektoriaus atstovai).

5. *Priemonės, skirtos kibernetinių incidentų prevencijai ir atsakui į juos.* Vertinant šią priemonių grupę taip pat pasigendama konkrečių, inovatyvių ir realiai įgyvendinamų pasiūlymų. Plane nurodoma, jog ketinama įgyvendinti TIS direktyvos nuostatas, kurti ir vystyti kibernetinių incidentų valdymo modelį. Pagirtinas siekis užtikrinti elektroninėje erdvėje vykdomų viešųjų pirkimų procedūrų saugumą, tačiau tai kol kas apsiriboja atitinkamu teisės aktų pakeitimu ar papildymu.

6. *Teisėkūros priemonės.* Numatoma nacionalinius teisės aktus suderinti su tarptautinių teisės aktų reikalavimais, ypač akcentuojamas TIS direktyvos nuostatų reikalavimų įgyvendinimas.

7. *Technologijų ir pramonės skatinimo priemonės.* Tai tiek saugumo standartus atitinkančių informacinių ir komunikacinių technologijų produktų sertifikavimas, konkurencingos rinkos kūrimas, remiant įmones, kuriančias ir diegiančias saugumo standartus atitinkančią produkciją, tiek Nacionalinės lyginamosios analizės laboratorijos, skirtos informacinių technologijų produktų tyrimams atlikti, įsteigimas.

Svarbu pažymėti, kad Nacionalinis kibernetinio saugumo centras Italijoje įsteigtas 2010 m., jis užsiima informavimu, konsultavimu, tyrimais ir glaudžiu bendradarbiavimu su privataus sektoriaus subjektais, keičiantis informacija apie kibernetinius incidentus ir jų prevenciją. Italijos Kibernetinio saugumo veiksmų plane numatyta papildomai įsteigti Nacionalinį kibernetinio saugumo vertinimo ir

[80] https://www.cyberwiser.eu/italy-it

sertifikavimo centrą. Šis centras įsteigtas 2019 m. Tai prie Ekonomikos plėtros ministerijos veikianti įstaiga, kurios pagrindinė funkcijas – vertinti informacinių technologijų sistemas, prekes ir paslaugas[81].

Kibernetinio saugumo veiksmų plane taip pat pažymima, kad sėkmingam jame numatytų priemonių įgyvendinimui svarbus žmogiškasis kapitalas, todėl būtinos investicijos į darbuotojų kvalifikacijos tobulinimą. Įdomu tai, kad privačios įmonės, kurių darbuotojų skaičius siekė 250 ir daugiau, 2018 – 2019 m. didino investicijas kibernetinio saugumo priemonėms įgyvendinti, tačiau 2020 m., matyt dėl COVID-19 pandemijos įtakos, 41 proc. tirtų įmonių investicijas sumažino[82].

Ispanija šiuo metu įgyvendina 2019 m. balandžio 30 d. patvirtintą kibernetinio saugumo strategiją[83], pakeitusią pirmąją 2013 m. šalies kibernetinio saugumo strategiją. 2013 m. strategija padėjo pagrindus kibernetinės erdvės pažeidžiamumų nustatymui ir veiksmų krypčių kibernetinio saugumo priemonėms įgyvendinti pasirinkimui, todėl 2019 m. strategija pagal joje suformuluotus tikslus ir jų įgyvendinimo priemones vertintina kaip tęstinė. Pastebėtina, kad 2013 m. strategijoje numatytos priemonės iš esmės buvo skirtos gynybai nuo kibernetinių incidentų, o 2019 m. strategijoje koncentruojamasi į prevencines priemones ir plėtrą.

Įgyvendindama 2013 m. strategijoje numatytas priemones, Ispanija atliko nemažai teisės aktų pakeitimų: tikslinta 2015 m. Nacionalinio saugumo strategija, į ją įtraukiant priemones, skirtas privataus sektoriaus subjektų informaciniams tikslams apsaugoti; atsižvelgiant į TIS direktyvos reikalavimus, 2018 m. rugsėjo 7 d. patvirtinta nauja Informacijos tinklų ir sistemų saugumo įstatymo redakcija; keistas Nacionalinio saugumo įstatymas, į jo nuostatas įtraukiant kibernetinio saugumo, kaip itin svarbios šalies saugumo srities, klausimų reguliavimą.

2019 m. strategijoje pažymima, kad kibernetinė erdvė, atverdama begales naujų galimybių, kartu kelia nemažai iššūkių, tokių kaip procesų robotizavimas, dirbtinis intelektas, daiktų internetas, tačiau Ispanija pajėgi juos įveikti ir yra pasiruošusi užimti vadovaujančias pozicijas formuojant kibernetinio saugumo politiką ne tik Europoje, bet ir pasaulyje. Kibernetinis saugumas vertintinas kaip viena iš prioritetinių valstybės veiklos sričių, kurioje būtinos sutelktos visų visuomenės narių pastangos. Strategijoje pripažįstama glaudaus bendradarbiavimo su privačiu sektoriumi būtinybė, o viena iš didžiausių problemų kibernetinio saugumo srityje nurodomas kvalifikuotų kibernetinio saugumo specialistų trūkumas.

Strategijoje nurodomos šios dvi esminės kibernetinio saugumo **grėsmių** grupės: kibernetinės atakos, kuriomis siekiama pažeisti techninę ar programinę įrangą, taip pat pasinaudoti saugomais

[81] Plačiau: https://atc.mise.gov.it/index.php/sicurezza/cvcn
[82] Šaltinis internete: https://www.statista.com/statistics/1202046/cybersecurity-budget-plan-italy/
[83] Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Spain.

duomenimis piktavališkais tikslais ir rimtesnio pobūdžio kibernetinės atakos, nukreiptos į elektroninę erdvę (joms priskiriami elektroniniai nusikaltimai, šnipinėjimas, hibridinės grėsmės).

Strategijos **vizija** *užtikrinti saugią ir patikimą kibernetinę erdvę, apsaugoti gyventojų teises ir laisves bei skatinti socialinį – ekonominį progresą* įgyvendinama per šiuos **tikslus**: 1) viešojo sektoriaus ir gyvybiškai svarbių paslaugų teikėjų informacinių ir komunikacinių tinklų bei sistemų saugumas ir atsparumas; 2) saugus ir patikimas kibernetinės erdvės naudojimas, jos apsauga nuo piktavališkų veiksmų; 3) verslo, socialinių ekosistemų ir piliečių apsauga nuo kibernetinių incidentų; 4) kibernetinio saugumo kultūros diegimas, žmogiškųjų ir technologinių išteklių plėtra; 5) tarptautinis bendradarbiavimas.

Pastebėtina, kad viešojo ir privataus sektorių bendradarbiavimo skatinimas neįtraukiamas į strategijoje suformuluotus tikslus. Tam tikri bendradarbiavimo aspektai pastebimi priemonių plane (pvz., koordinuoti teisėsaugos pareigūnų, valdžios institucijų ir gyventojų veiksmai, užkertant kelią elektroniniams nusikaltimams), tačiau esminės reikšmės jiems neteikiama, nes minėti klausimai iš esmės išspręsti įgyvendinant 2013 m. strategijoje numatytas priemones. Taip pat strategijoje neužsimenama apie kibernetinio saugumo priemones įgyvendinančių specializuotų institucijų steigimą, nes tai taip pat įgyvendinta. Įsteigtas Nacionalinis kibernetinio saugumo institutas[84], kurio veikla orientuota į vadovavimą įvairioms kibernetinio saugumo iniciatyvoms, keitimąsi informacija su visais suinteresuotais subjektais, inovacijų skatinimu, bendradarbiavimu su kibernetinio saugumo institucijomis nacionaliniu ir tarptautiniu lygmeniu. Be to, veikia Nacionalinis infrastruktūros apsaugos ir kibernetinio saugumo centras[85], atsakingas už veiklos, susijusios su ypatingos svarbos infrastruktūros objektų apsauga, priežiūrą ir koordinavimą, Nacionalinis kriptologijos centras.

Įgyvendinant tikslus laikomasi šių **principų:** bendradarbiavimo (viešojo ir privatus sektorių bei visos visuomenės), prognozavimo (prevencija svarbesnė, nei kova su pasekmėmis), efektyvumo ir atsparumo.

Aptarsiu įdomesnes ar inovatyviausias kibernetinio saugumo užtikrinimui skirtas priemones, numatytas strategijoje.

1. *Priemonės, skirtos informacinių ir komunikacinių tinklų ir sistemų apsaugai*: ypač akcentuojamas darbuotojų analitinių gebėjimų tobulinimas, bendradarbiavimas su mokslinių tyrimų centrais. Pabrėžiama keitimosi informacija platformų svarba, numatoma šių platformų specializacija pagal veiklos sritis. Numatoma parengti saugių, sertifikuotų informacinių technologijų produktų katalogus ir užtikrinti, kad kritinės svarbos infrastruktūrose būtų naudojami tik į katalogus įtraukti produktai.

[84] Plačiau: https://www.incibe.es/en
[85] Plačiau: http://www.cnpic.es/en/index.html

2. *Priemonės, skirtos saugiam ir patikimam kibernetinės erdvės naudojimui.* Priemonės orientuotos tiek į teisėkūrą (elektroninių nusikaltimų sąrašo išplėtimą, teisėsaugos įgaliojimų nustatymą), tiek į teisėsaugos pajėgumų didinimą (specialūs kvalifikacijos kėlimo kursai, papildomų etatų skyrimas). Be to, ieškoma galimybių keistis informacija su privataus sektoriaus subjektais (šiuo atveju keitimasis labiau vienpusis, policija neinformuoja apie vykdomus tyrimus, tačiau gali teikti konsultacijas).

3. *Verslo, ekosistemų ir piliečių apsaugos elektroninėje erdvėje priemonės:* inovacijos elektroninės autentifikacijos procese; platformų, kuriose galima pranešti apie patirtus kibernetinius incidentus ir gauti kvalifikuotą konsultaciją, diegimas. Numatomi specializuoti mokymai, galimybių dirbti su tam tikromis elektroninėmis sistemomis suteikimas, tik išklausius atitinkamus mokymus ir gavus sertifikatą.

4. *Kibernetinio saugumo kultūros diegimo priemonės.* Šioje srityje iš esmės visos priemonės orientuotos į visų visuomenės narių grupių mokymus apie saugų elgesį elektroninėje erdvėje. Įdomu tai, kad į mokymų procesą ketinama įtraukti žiniasklaidos atstovus, kurie galėtų suteikti kvalifikuotas konsultacijas, kaip atskirti netikras naujienas ar dezinformaciją.

5. *Priemonės, skirtos tarptautiniam bendradarbiavimui stiprinti.* Priemonės apima dalyvavimą tarptautiniuose forumuose, konferencijose, taip pat tarptautinių teisės aktų nuostatų įgyvendinimą. Pažymima dalijimosi gerąja patirtimi būtinybė nustatant ir imantis priemonių prieš hibridines kibernetines atakas.

Strategijoje įvardijami už numatytų priemonių įgyvendinimą atsakingi subjektai, pateikiama jų bendradarbiavimo ir veiksmų koordinavimo schema.

Apibendrinant galima daryti išvadą, kad Ispanijos 2019 m. kibernetinio saugumo strategija parengta įvertinus problemas, su kuriomis buvo susidurta įgyvendinant ankstesnę strategiją, ir jau atlikus nemažai kibernetinio saugumo įgyvendinimui svarbių veiksmų: įsteigus atsakingas institucijas, pasiekus gerų rezultatų bendradarbiavimo su privataus sektoriaus subjektais srityje, įdiegus specializuotas mokymosi programas ir keitimosi informacija platformas. Vis tik strategija nepasižymi išskirtiniu originalumu ir numatytų priemonių išskirtinumu. Ji galėtų būti geru pavyzdžiu valstybėms, kuriančioms ir įgyvendinančioms pirmąsias kibernetinio saugumo strategijas, tačiau nesiekia jau nagrinėtų Vokietijos, Jungtinės Karalystės ir Australijos kibernetinio saugumo strategijų lygmens.

Pažymėtina ir tai, kad Ispanija negali pasigirti ženkliai pagerėjusia kibernetinio saugumo būkle. „BitSight“ tyrėjai nustatė[86], kad Ispanijos įmonės, lyginant su kitų Europos šalių įmonėmis, lėčiau sureaguoja į kibernetinius incidentus (16 proc. atvejų) ir sprendžia incidentus 1,5 para ilgiau. Be abejo, tai tik vieni iš daugelio atliekamų tyrimų, todėl jų rezultatai vertintini kaip tam tikros tendencijos.

[86] Šaltinis internete: https://business.blogthinkbig.com/cyber-risk-spain-cybersecurity/

Pirmoji Portugalijos kibernetinio saugumo strategija buvo priimta 2015 m. gegužės 28 d.[87] ir galiojo trejus metus. Jos tikslas – *gerinti tinklų ir informacijos saugumą, saugoti ypatingos svarbos informacijos infrastruktūros objektus, užtikrinti nemokamą, saugų ir efektyvių kibernetinės erdvės naudojimą visiems piliečiams, viešojo ir privataus sektoriaus subjektams* būdingas panašiu laikotarpiu (2013 – 2015 m.) kurtoms ir diegtoms nacionalinėms kibernetinio saugumo strategijoms.

Pažymima, kad strategijoje numatytų priemonių įgyvendinimas grindžiamas penkiais pamatiniais **principais**: *subsidiarumo* (kibernetinės erdvės saugumas traktuojamas kaip sudėtinė nacionalinio saugumo dalis. Valstybė nustato esminius reikalavimus saugiam naudojimuisi kibernetine erdve užtikrinti, o privataus sektoriaus subjektai ir gyventojai prisideda prie jų įgyvendinimo); *vientisumo* (pažymima, kad kibernetine erdve naudojasi tiek civiliai, tiek kariškiai, tiek viešasis, tiek privatus sektorius, tiek asmenų grupės, tiek atskiri individai, todėl visų jų veiksmai ir pastangos turi būti suderinti); *bendradarbiavimo* (tiek nacionalinio, tiek tarptautinio), *proporcingumo* (kibernetinei erdvei kylančios rizikos tinkamai įvertinamos ir adekvačiai išsprendžiamos) ir *sąmoningumo* (techninės priemonės neveikia, jei vartotojai nesilaiko saugumo reikalavimų).

Strategijoje suformuluoti keturi **tikslai**: 1) skatinti ir vystyti saugų, nemokamą ir efektyvų naudojimąsi kibernetine erdve; 2) apsaugoti pagrindines asmens teises ir laisves, saviraiškos laisvę, asmens duomenis ir privatumą; 3) stiprinti kibernetinės erdvės atsparumą grėsmėms, apsaugoti kritinės infrastruktūros ir gyvybiškai svarbias paslaugas teikiančius objektus; 4) kibernetinę erdvę paversti ekonomikos ir inovacijų augimo vieta. Tikslams įgyvendinti numatytos **priemonės** suskirstytos į šešias grupes:

1. Skirtos kibernetinio saugumo struktūros suformavimui. Pažymima, kad kibernetinei erdvei kylančių grėsmių sudėtingumas reikalauja aiškios, lanksčios ir gerai koordinuotos struktūros, gerų rezultatų pasiekti neįmanoma, jei su kibernetinėmis grėsmėmis bandys tvarkytis tarpusavyje nesusiję ir skirtingas funkcijas įgyvendinantys subjektai. Dėl šios priežasties būtina: parengti veiksmų ir įgaliojimų planą, nustatant, kad visos kibernetinį saugumą įgyvendinančios institucijos bus atskaitingos Ministrui Pirmininkui. Be to, numatyta stiprinti Nacionalinio kibernetinio saugumo centro įgaliojimus[88] ir vystyti kibernetinės gynybos pajėgumus, tobulinti dalijimosi informacija apie kibernetines grėsmes ir gerąją praktiką jas sprendžiant platformų veiklą, steigti kibernetinių krizių valdymo tarnybą bei teisiškai reglamentuoti kibernetinės erdvės valdymo procesus;

2. Skirtos kovai su elektroniniais nusikaltimais. Numatoma tiek atnaujinti baudžiamuosius įstatymus, aiškiai aprašant elektroninių nusikaltimų požymius, tiek imtis priemonių tyrėjų, tiriančių

[87] Prieiga internetu: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Portuguese_National_Cyberspace_Security_Strategy_EN.pdf

[88] Portugalijos nacionalinis kibernetinio saugumo centras įsteigtas 2014 m., jo įgaliojimų apimtis nuolat plečiama. Šaltinis internete: Mission and competences » About us » Centro Nacional de Cibersegurança EN (cncs.gov.pt)

tokio pobūdžio nusikalstamas veikas, kvalifikacijai tobulinti. Pertvarkoma Portugalijos kriminalinės policijos struktūra, gerinamas jos techninis aprūpinimas bei steigiami papildomi etatai;

3. Orientuotos į kibernetinės erdvės ir kritinės reikšmės infrastruktūros apsaugą. Tai iš esmės techninio pobūdžio priemonės, padedančios aptikti bandymus įsilaužti į informacines sistemas ir operatyviai į juos reaguoti. Nepamirštamas ir žmogiškasis faktorius – siekiama, kad duomenų bazėse esanti ypatingos svarbos informacija būtų prieinama tik įgaliotiems asmenims. Kuriama ir diegiama Nacionalinė informacijos infrastruktūros apsaugos sistema;

4. Švietimo ir prevencijos priemonės. Ypatingas dėmesys skiriamas viešųjų įstaigų darbuotojams ir ypatingos svarbos infrastruktūros objektuose dirbantiems specialistams, tačiau saugaus elgesio elektroninėje erdvėje programos diegiamos ir į pradinio, vidurinio bei aukštojo mokslo programas, specializuoti mokymai numatomi vyresnio amžiaus asmenims ir kitoms elektroninėje erdvėje itin pažeidžiamoms socialinėms grupėms, taip pat smulkių ir vidutinių įmonių darbuotojams bei savarankiškai dirbantiems asmenims;

5. Į mokslo ir technologijų plėtrą orientuotos priemonės. Numatoma teikti paramą moksliniams tyrimams ir iniciatyvoms, bendradarbiauti su akademine bendruomene, pramonės įmonėmis. Ypač skatinimas šalies mokslininkų dalyvavimas tarptautiniu mastu atliekamuose tyrimuose;

6. Skirtos tarptautinio bendradarbiavimo stiprinimui. Šios grupės priemonės įprastinės tokio pobūdžio priemonėms, tai dalyvavimas tarptautiniuose forumuose ir diskusijose, vykimas į tarptautines kibernetines pratybas. Numatomas ne tik pasyvus dalyvavimas, bet ir įvairių iniciatyvų kibernetinės gynybos, terorizmo, elektroninių nusikaltimų prevencijos klausimais.

Numatoma kasmet peržiūrėti išsikeltus strateginius tikslus, esant poreikiui – juos performuluoti, taip pat reguliariai peržiūrėti numatytų priemonių vykdymo rezultatus.

Šios, šiuo metu jau iš dalies įgyvendintos ir kitu dokumentu (2019 m. strategija) pakeistos strategijos apžvalgai darbe buvo skirta daugiau dėmesio, nes ji laikytina puikiu pavyzdžiu, rodančiu, kad jau pirmajame nacionaliniame valstybės kibernetinio saugumo dokumente įmanoma tinkamai sureguliuoti esminius klausimus – tiek inovatyvių technologinių priemonių diegimą, tiek valstybės institucijų, dirbančių kibernetinio saugumo srityje, kompetencijų ir atsakomybių klausimus, tiek bendradarbiavimą, švietimą ir kitus svarbius aspektus.

Šiuo metu Portugalija įgyvendina 2019 m. birželio 6 d. kibernetinio saugumo strategiją[89]. Tai taip pat pakankamai trumpas ir konkretus dokumentas (vertimas į anglų kalbą užima 7 puslapius), savo struktūra iš esmės nesiskiriantis nuo 2015 m. strategijos. Strategija parengta 2019—2023 m. laikotarpiui. Joje pažymima, kad didėjant kibernetinių išpuolių skaičiui, išpuoliams sudėtingėjant,

[89] Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Portugal

būtina įvertinti vykdomos prevencijos veiksmingumą, iš naujo apsvarstyti būdus ir priemones kibernetiniam saugumui stiprinti. Būtinybę ieškoti naujų inovatyvių prevencijos būdų skatina ir visuomenės kompiuterizacija, užvaldančia praktiškai visas gyvenimo sritis.

Strategijoje suformuluota **vizija** iki 2023 m. tapti saugia ir klestinčia valstybe, gebančia inovatyviais ir kibernetiniams išpuoliams atspariais veiksmais užtikrinti pagrindines žmogaus teises ir laisves, saugų institucijų funkcionavimą, atitinkantį visuomenės skaitmeninės evoliucijos iššūkius.

Strateginių **tikslų** skaičius sumažėjo iki trijų: 1) *kibernetinės erdvės atsparumo išpuoliams ir nepageidaujamai intervencijai didinimas* (ypač akcentuojama valstybinės reikšmės interesų ir kritinės svarbos infrastruktūrų apsauga); 2) *inovacijų skatinimas* ir 3) *išteklių kibernetinės erdvės saugumui užtikrinti telkimas* (omenyje turimi ne tik finansiniai, bet ir informaciniai bei žmogiškieji resursai). Tikslams įgyvendinti strategijoje numatytų **priemonių** skirstymas į šešias grupes išlieka. Aptarsiu svarbesnes ir inovatyviausias priemones:

1. Institucinės kibernetinės erdvės saugumo stiprinimo priemonės: dar kartą plečiami Nacionalinio kibernetinio saugumo centro įgaliojimai, suteikiant jam tarptautinio bendradarbiavimo su užsienio valstybių teisėsaugos institucijomis kibernetinio saugumo srityje koordinavimo funkciją. Prokuratūros sistema pertvarkoma, steigiant atskirus elektroninių nusikaltimų tyrimo padalinius. Kriminalinės policijos pajėgumai stiprinami per aprūpinimą reikiamomis technologijomis ir papildomus etatus;

2. Švietimo ir sąmoningumo ugdymo priemonės: numatoma detaliai išanalizuoti kibernetinių nusikaltėlių psichologinius portretus, tikslus, veikimo būdus ir parengti atsakomąsias priemones į tipiniais laikomus kibernetinius išpuolius. Taip pat ieškoma naujų, inovatyvių būdų vaikų, paauglių ir garbaus amžiaus asmenų švietimui apie saugų elgesį elektroninėje erdvėje. Sektinu pavyzdžiu laikytina tai, kad švietimas vertinamas kaip tęstinis procesas, neapsiribojama paskaitos išklausymu ar supažindinimu su atitinkamomis instrukcijomis. Įdomu ir tai, kad ieškoma būdų kuo anksčiau nustatyti jaunuolių gabumus kibernetinio saugumo užtikrinimo srityje ir juos skatinti rinktis atitinkamas profesijas;

3. Techninės kibernetinės erdvės saugumo stiprinimo priemonės: itin naujų priemonių nenumatyta. Pažymėtina tik tai, kad į kibernetinės erdvės saugumo stiprinimo veiklą ketinama įtraukti ir smulkiąsias įmones;

4. Kovos su kibernetiniais nusikaltimais priemonės: viena iš numatytų priemonių – teisėsaugos pareigūnų mokymai atpažinti neteisėtus veiksmus elektroninėje erdvėje ir nedelsiant į juos reaguoti. Taip pat pabrėžia būtinybė atnaujinti teisės aktus ir skatinti teisėsaugos institucijas glaudžiau bendradarbiauti tarpusavyje, keistis aktualia informacija, ieškoma būdų įteisinti naujus operatyvinius veiksmus, tokius kaip elektroninio susirašinėjimo stebėjimas realiu laiku;

5. Priemonės tyrimų ir inovacijų srityje. Kaip ir ankstesnėje, 2015 m. strategijoje, ypač skatinamas mokslininkų dalyvavimas tarptautiniuose projektuose, taip pat technologijų, naudotinų tiek kariniais, tiek civiliniais tikslais, kūrimas.

Viena iš įgyvendintų technologinių naujovių – 2019 m. sausio mėn. sudaryta inkubatoriaus „StartUp Lisboa“ bendradarbiavimo sutartis su „Bright Pixel“. Partnerystės tikslas – padėti augti B2B startuoliams kibernetinio saugumo srityje bei bendradarbiauti su besivystančiomis „blockchain“ bei dirbtinio intelekto technologijas kuriančiomis įmonėmis[90].

6. Nacionalinis ir tarptautinis bendradarbiavimas: apsieinama be garsių šūkių apie lyderystę ir vadovavimą, apsiribojama *prisidėjimu* prie tarptautinės kibernetinio saugumo politikos formavimo.

Strategijoje numatytų priemonių įgyvendinimas peržiūrimas ne rečiau kaip kartą per metus, esant poreikiui priemonės performuluojamos ar jų atsisakoma.

Įdomu pastebėti, kad vadovaujantis Jungtinių Tautų Tarptautinės telekomunikacijų sąjungos parengtais Globalaus kibernetinio saugumo indekso nustatymo kriterijais, 2020 m. Portugalija geriausių rezultatų pasiekė kibernetinio saugumo politikos įgyvendinimo, švietimo ir profesinio rengimo, asmens duomenų apsaugos ir kovos su elektroniniais nusikaltimais srityse. Labiausiai pasistengti reikėtų užtikrinant kritinės svarbos infrastruktūros apsaugą ir valdant kibernetinio saugumo krizes[91].

Apibendrinant Portugalijos 2015 m. 2019 m. kibernetinio saugumo strategijas galima teigti, kad nepaisant tam tikrų trūkumų (pvz., subjektų, atsakingų už atskirų priemonių įgyvendinimą, neįvardijimo) tai tinkamai parengti dokumentai, atitinkantys TIS direktyvos ir Europos Sąjungos komisijos 2017 m. spalio 4 d. komunikato priede „Racionaliausias tinklų ir informacijos saugumas“ nustatytus reikalavimus.

[90] Plačiau internete: https://portugalstartups.com/2019/01/startup-lisboa-bright-pixel-partner/.
[91] Šaltinis internetu: https://www.ncsi.ega.ee/country/pt/.

3. LIETUVOS KIBERNETINIO SAUGUMO STRATEGINIŲ DOKUMENTŲ VERTINIMAS

3.1 Pirmieji dokumentai, skirti kibernetinio saugumo klausimų reglamentavimui

Lietuva kibernetinio saugumo įgyvendinimo, kibernetinio saugumo politikos formavimo ir kibernetinio saugumo priemonių diegimo procese nėra naujokė ir daliai valstybių gali būti sektinu pavyzdžiu. Teigti, jog viskas sekasi puikiai ir neturime, kur tobulėti, būtų per drąsu, bet tam tikri rodikliai kalba patys už save.

194 valstybes vienijanti Jungtinių Tautų Tarptautinė telekomunikacijų sąjunga kasmet įvertina valstybių pajėgumus kibernetinio saugumo srityje (nacionalinė teisėkūra, bendradarbiavimas, atitinkamų techninių ir organizacinių reikalavimų įgyvendinimą) ir skelbia Globalų kibernetinio saugumo indeksą. Iš 57-tos vietos 2017 m. Lietuva pakilo į 4-ąją vietą 2019 m., nusileisdama tik Prancūzijai, Jungtinėms Amerikos Valstijoms ir Jungtinei Karalystei[92].

Pirmieji žingsniai kibernetinio saugumo teisėkūroje nebuvo paprasti. Lietuvos Respublikos Vyriausybė 2001 m. gruodžio 22 d. nutarimu Nr. 1625 „Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo“[93] patvirtino *Informacijos technologijų saugos valstybinę strategiją ir jos įgyvendinimo planą*. Šis dokumentas pagal paskirtį ir teisinio reglamentavimo turinį gali būti laikomas pirmąja Lietuvos strategija kibernetinio saugumo srityje.

Dokumentas nesudėtingas, juo siekiama plėtoti informacijos technologijų saugos teisinį reglamentavimą, stiprinti svarbiausiųjų valstybės informacinių sistemų saugą, plėtoti metodologinę ir konsultacinę sistemą, ugdyti valstybės tarnautojų ir duomenų saugos įgaliotinių įgūdžius informacinių technologijų saugos srityje. Strategijoje nustatyti informacijos technologijų saugos plėtojimo principai (informacijos technologijų saugos sistemos ir informacinių sistemų tarpusavio priklausomybės, aplinkos stebėjimo, saugos užtikrinimo pagal informacijos svarbą, informacinių technologijų naudotojų ir specialistų švietimo) bei įgyvendinimo kryptys (numatoma steigti informacijos technologijų saugos įvertinimo (konsultavimo) padalinį, užtikrinti, kad duomenys būtų perduodami tik saugiu valstybiniu duomenų perdavimo tinklu, rūpintis interneto tarnybinių stočių sauga valstybės institucijose, nustatyti jų pažeidžiamumą).

Strategijos įgyvendinimo plane numatytos šešios priemonės, kurias ketinama įgyvendinti 2002–2004 metais, pažymėtina, kad jų įgyvendinimas kainuos 3265 tūkst. litų. Pagal įvardytus tikslus numatytos šios **priemonės:** 1) parengti Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d.

[92] Lithuania takes the 4th position in the Global Cybersecurity Index. LtLife.lt, 2019 m. balandžio 2 d. publikacija: https://ltlife.lt/lt-life-english/lithuania-takes-the-4th-position-in-the-global-cybersecurity-index/

[93] Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.157225?jfwid=32wf55g0

nutarimo Nr. 952 „Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose“ dalinio pakeitimo projektą, suklasifikuoti informaciją pagal duomenų grupes, parengti lietuviškus informacijos technologijų saugos standartus; 2) įvertinti valstybės institucijų informacijos technologijų saugą ir sukurti saugų valstybinį duomenų perdavimo tinklą, įgyvendinti asmens tapatybės nustatymo priemones bei užtikrinti interneto tarnybinių stočių saugą valstybės institucijose; 3) parengti informacijos technologijų saugos atitikties vertinimo planus, tvarką, kriterijus ir metodinę medžiagą; 4) parengti Informacijos technologijų saugos mokymo programą viešojo administravimo institucijoms; 5) rengti informacijos technologijų saugos specialistus; 6) įsteigti informacijos technologijų saugos įvertinimo (konsultavimo) padalinį bei padalinį Saugumo priežiūros tarnybos funkcijoms vykdyti.

Bendradarbiavimo su privačiu sektoriumi sritis šioje strategijoje neaptariama, už plane numatytų priemonių įgyvendinimą atsakingos Vidaus reikalų, Aplinkos ir Švietimo ir mokslo ministerijos. Svarbu ir tai, kad įgyvendinant šią strategiją priimta nemažai informacijos saugos klausimus reglamentuojančių teisės aktų[94] ir daugiau kaip 30 informacinių sistemų duomenų saugos nuostatų, pradėtas organizuoti saugos įgaliotinių mokymas, Vidaus reikalų ministerijoje įsteigtas informacinių technologijų saugą valstybės institucijose koordinuojantis padalinys.

Kitas Lietuvos strateginis dokumentas kibernetinio saugumo srityje – Lietuvos Respublikos Vyriausybės 2006 m. birželio 19 d. nutarimu Nr. 601 „Dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo“[95] patvirtinta *Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 metų.*

Svarbu pažymėti tai, kad strategijoje pateiktos saugos įgaliotinio ir elektroninės informacijos saugos incidento sąvokos. Elektroninės informacijos saugos incidentas apibrėžiamas taip: „įvykis ar veiksmas, kuris gali sudaryti neteisėto prisijungimo prie informacinės sistemos galimybę, sutrikdyti ar pakeisti informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti“. Taip pat įdomu tai, kad strategijoje nurodomos elektroninės informacijos saugos informacinėse sistemos stipriosios (saugos užtikrinimo koordinavimas, nuotolinio saugos mokymo sistemos įdiegimas, sukurti saugaus informacijos perdavimo tarp informacinių sistemų infrastruktūros pagrindai) ir silpnosios (kvalifikuotų elektroninės informacijos saugos specialistų trūkumas, koordinuoto bendradarbiavimo tarp viešojo ir privataus

[94] Vidaus reikalų ministro 2003 m. liepos 16 d. įsakymas Nr. 1V-272 „Dėl Tipinių duomenų saugos nuostatų patvirtinimo“, 2004 m. gegužės 6 d. įsakymas Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo, 2004 m. gegužės 21 d. įsakymas Nr. 1V-176 „Dėl Interneto tarnybinių stočių apsaugos rekomendacijų patvirtinimo“, pakeistas ir nauja redakcija išdėstytas Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimas Nr. 952 „Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose“.

[95] Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.278475?jfwid=fhhu5mn3t

sektorių subjektų trūkumas, išankstinio perspėjimo apie galimas grėsmes ir reagavimo į saugos incidentus sistemos nebuvimas, lėšų elektroninės informacijos saugai užtikrinti trūkumas) vietos.

Tikslai suformuluoti strategijos 9 punkte: tobulinti elektroninės informacijos saugos koordinavimą ir priežiūrą, teisiškai reguliuoti elektroninės informacijos saugą, kelti saugos kultūrą, tobulinti elektroninės informacijos perdavimo infrastruktūros saugą ir skatinti elektroninės informacijos saugos užtikrinimo projektų įgyvendinimą (tikslo įgyvendinimui numatoma pasitelkti privataus sektoriaus atstovus). Priemonių plane numatyta 19 **priemonių**, paminėsiu aktualiausias: kovos su elektroniniais nusikaltimais padalinio įsteigimas; standartizacijos procesų tobulinimas (perimami tarptautinių standartizacijos organizacijų elektroninės informacijos saugos standartai); Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimų parengimas ir patvirtinimas; švietimo kibernetinio saugumo srityje priemonės (informacijos apie elektroninės informacijos saugą ir elektroninei informacijai kylančias grėsmes skelbimas interneto tinklalapyje www.esaugumas.lt[96] kompaktinių plokštelių ir informacinių bukletų saugaus elgesio elektroninėje erdvėje parengimas ir platinimas, bendrojo ugdymo ir profesinio mokymo programų papildymas elektroninės informacijos saugos temomis ir rekomendavimas aukštosioms mokykloms šiomis temomis papildyti savo studijų programas).

Atsakingų už plane numatytų priemonių įgyvendinimą institucijų padaugėjo, be jau minėtų ministerijų priemones įgyvendinti pavesta Susisiekimo ministerijai, Policijos departamentui prie Vidaus Reikalų ministerijos, Standartizacijos departamentui prie Aplinkos ministerijos, Ryšių reguliavimo tarnybai ir Informacinės visuomenės plėtros komitetui prie Lietuvos Respublikos Vyriausybės.

Dar vienas Lietuvos strateginis dokumentas kibernetinio saugumo srityje – Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796 patvirtinta *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011 – 2019 metais programa*[97], kurios analizei skirtas kitas šio darbo poskyris.

3.2 Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos analizė

Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011 – 2019 metais programoje (toliau šiame poskyryje – Programa), skirtingai nuo ankstesnių strateginių dokumentų,

[96] Tinklalapis šiuo metu veikia ir jame gausu aktualios informacijos saugumo elektroninėje erdvėje klausimais.
[97] Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.403385

išsikeltas **strateginis tikslas** – plėtoti elektroninės informacijos saugą, užtikrinti kibernetinį saugumą[98], kad 2019 m. elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 procentus visų valstybės informacinių išteklių, vidutinis ypatingos svarbos informacinės infrastruktūros incidentų likvidavimo laikas sumažėtų iki 0,5 valandos, o gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis pasiektų 60 procentų. Strateginis tikslas suformuluotas ambicingai, tačiau trūksta gilesnės analizės, dėl kokios priežasties pasirinkti būtent šie kriterijai.

Programoje pateikiama incidento sąvoka šiek tiek platesnė nei Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinėje strategijoje pateikta elektroninės informacijos saugos incidento sąvoka, dokumente taip pat nurodoma, kas laikoma ypatingos svarbos informacine infrastruktūra (tai elektroninių ryšių tinklas, informacinė sistema ar informacinių sistemų grupė, kurioje įvykęs incidentas padaro ar gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui ar visuomenės gerovei). Žalos dydžio nustatymo kriterijai nepateikiami.

Tikslai trys:

1. *Užtikrinti valstybės informacinių išteklių saugumą*. Pažymėtina, kad Programoje nurodoma, jog kibernetinės erdvės saugumu suinteresuoti visi subjektai, kurių veikla susijusi su joje teikiamomis paslaugomis (valstybės institucijos, privatūs ūkio subjektai, akademinė bendruomenė ir kiti), todėl neaišku, kodėl siekiama apsaugoti tik valstybės informacinius išteklius ir kodėl informaciniai ištekliai tapatinami su kibernetinės erdvės saugumu.

2. *Užtikrinti veiksmingą ypatingos svarbos informacinės infrastruktūros funkcionavimą*. Tikslą planuojama įgyvendinti per beveik identiškai suformuluotą uždavinį: užtikrinti ypatingos svarbos informacinės infrastruktūros saugumą. Tai kritikuotina formuluotė, nes vien saugumo priemonių įgyvendinimas neduoda jokių garantijų dėl funkcionavimo.

3. *Užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje*. Tai ketinama įgyvendinti per apsaugą nuo kibernetinių atakų, kiberneteinėje erdvėje teikiamų paslaugų saugumą, kibernetinio saugumo kultūros vystymą.

Numatyta, kad Programos įgyvendinimą koordinuoja Vidaus reikakų ministerija, kuriai visi joje numatytas priemones įgyvendinantys subjektai kasmet iki vasario 1 d. privalo pateikti informaciją apie vykdytas priemones ir pasiektus rezultatus. Be to, Lietuvos Respublikos Vyriausybės 2012 m. balandžio 25 d. nutarimu Nr. 468[99] pakeista Elektroninės informacijos saugos (kibernetinio saugumo) koordinavimo komisijos sudėtis ir patvirtinti šios komisijos nuostatai.

Į Programoje numatytas priemones įgyvendinančių subjektų ratą įtraukta Ministro Pirmininko tarnyba, Krašto apsaugos, Ūkio, Energetikos, Finansų ministerijos, Valstybinė duomenų apsaugos

[98] Programoje pateiktos sąvokos „elektroninės informacijos saugumas“ ir „kibernetinis saugumas“ (3 punkte, 6.1, 6.3 papunktyje ir kitur) vartojamos kaip sinonimai, nors jų reikšmė skiriasi.
[99] Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.423375?jfwid=g979e52t4

inspekcija, Lietuvos mokslo ir studijų institucijų kompiuterinio tinklo (LITNET) taryba, Valstybės saugumo departamentas ir viešojo administravimo institucijos, teikiančios paslaugas kibernetinėje erdvėje. Programoje pastebimo bendradarbiavimo su privačiu sektoriumi užuomagos. Privataus sektoriaus subjektai nėra įtraukiami į joje numatytas priemones įgyvendinančių subjektų sąrašą kaip lygiaverčiai partneriai, tačiau Programos įgyvendinimo vertinimo kriterijų ir siekiamų jų reikšmių lentelės 22 punkte užsimenama apie *bendradarbiavimą* su privačiu sektoriumi įgyvendinant kibernetinio saugumo projektus.

Pagirtina tai, kad numatytų priemonių įgyvendinimo rodikliai nustatyti 2011, 2015 ir 2019 metams, tačiau vertinimo kriterijų formulavimas kelia pagrįstų abejonių, dalis kriterijų neturi pradinės atskaitos taško, pvz., nurodoma, kad Lietuvos gyventojų pasitikėjimo kibernetinėje erdvėje teikiamomis paslaugomis lygis, procentais 2015 m. sieks 50, o 2019 – 67 proc. Atskaitos taškas (kiek gyventojų pasitikėjo kibernetinėje erdvėje teikiamomis paslaugomis Programos priėmimo metu) neaiškus, jo nustatymo kriterijai nenurodyti.

Nemaža dalis priemonių suformuluota pernelyg abstrakčiai, todėl jų įgyvendinimas ar neįgyvendinimas sunkiai pamatuojamas. Pvz., Programos įgyvendinimo vertinimo kriterijų ir siekiamų jų reikšmių lentelės 42 punkte suformuluota priemonė „Kelti elektroninės informacijos saugos (kibernetinio saugumo) kultūrą“ vertinama per Lietuvos gyventojų, suvokiančių kibernetinio saugumo principus, procentinę dalį. Neaišku, kokiame teisės akte (nacionaliniame ar tarptautiniame) įtvirtintus principus gyventojai turėtų suvokti, kaip nustatomas jų suvokimas ir pan.

2015 m. gruodžio 9 d. Valstybinio audito ataskaitoje Nr. VA-P-90-4-16 „Kibernetinio saugumo aplinka Lietuvoje“ nurodoma, kad kibernetinio saugumo būklė Lietuvoje negerėja, o Programa, kurioje numatytomis priemonėmis planuota pasiekti daugiausia rezultatų šioje srityje, vykdoma nerezultatyviai[100]. 2015 m. rugsėjo mėn. buvo pasiekta tik 23 proc. planuotų rodiklių (iš viso Programoje numatyti 59 rodikliai), 48 proc. pasiekti iš dalies, 29 proc. – nepasiekta. Audito ataskaitoje prognozuojama, kad 2015 m. nebus pasiektas nė vienas Programoje numatytas tikslų rodiklis, o bendras Programos tikslų įgyvendinimas audito atlikimo metu siekė tik 21 proc. Be to, atkreiptas dėmesys į neefektyvų Programos koordinavimą ir ją įgyvendinančių įstaigų nepakankamą aktyvumą, ką įtakojo tarpinstitucinio veiklos plano neparengimas, neefektyvus Programos koordinavimas ir ją įgyvendinančių subjektų nepakankamas aktyvumas. Atkreiptas dėmesys į tai, kad Vidaus reikalų ministerija neinicijavo Programos nuostatų atnaujinimo, nors jos įgyvendinime dalyvaujančios institucijos 2012–2015 m. tokius siūlymus teikė.

[100] 2015 m. gruodžio 9 d. Valstybinio audito ataskaita Nr. VA-P-90-4-16 „Kibernetinio saugumo aplinka Lietuvoje“, P. 7.

Programa galiojo iki 2018 m. rugpjūčio 13 d.[101], kol ją pakeitė Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 patvirtinta Nacionalinė kibernetinio saugumo strategija[102].

3.3 2018–2023 m. Nacionalinės kibernetinio saugumo strategijos ypatumai ir joje numatytų priemonių įgyvendinimo problemos

Lietuvos Nacionalinė kibernetinio saugumo strategija parengta penkerių metų laikotarpiui ir turi būti įgyvendinta iki 2023 m. įskaitytinai. Prieš pradedant analizuoti jos turinį, būtina aptarti Lietuvos Respublikos kibernetinio saugumo įstatymo[103] (toliau šiame poskyryje – Įstatymas) nuostatas jau vien dėl to, kad strategijoje remiamasi pamatinėmis Įstatyme suformuluotomis sąvokomis, tokiomis kaip kibernetinė erdvė, kibernetinis saugumas, kibernetinis incidentas ir kitos. Be to, Įstatyme numatyti principai, kuriais grindžiamas kibernetinis saugumas, valstybės institucijų įgaliojimai kibernetinio saugumo srityje. Įstatymo 5 straipsnio 1 dalies 1 punkte nurodoma, kad Nacionalinę kibernetinio saugumo strategiją tvirtina Vyriausybė, o jos rengimą koordinuoja Krašto apsaugos ministerija (6 straipsnio 1 dalies 1 punktas). Svarbu ir tai, kad šiame teisės akte apibrėžti kibernetinio saugumo užtikrinimo būklę analizuojančios ir pasiūlymus dėl jos gerinimo teikiančios Kibernetinio saugumo tarybos įgaliojimai ir Nacionalinio kibernetinio saugumo centro funkcijos, įgyvendinant kibernetinio saugumo politiką.

Įstatymas priimtas 2014 m. gruodžio 11 d., nauja redakcija išdėstytas 2018 m. birželio 27 d. Naujoje Įstatymo redakcijoje aiškiau apibrėžtos ypatingos svarbos informacinės infrastruktūros ir kibernetinės erdvės sąvokos, tikslintas kibernetinio incidento apibrėžimas (aiškiai nurodoma veikos sfera – kibernetinė erdvė, taip pat tiksliau apibrėžiamos pačios veikos, laikytinos kibernetiniais incidentais ir jų pasekmės (potenciali ar reali grėsmė arba neigiamas poveikis). Pateiktos debesijos paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų sąvokos.

Atitinkamos nuostatos suformuluotos įgyvendinant TIS direktyvos reikalavimus, įtraukta nauja kibernetinio saugumo subjektų – skaitmeninių paslaugų teikėjų – kategorija, nurodytos jų pareigos. Be to, koreguota kibernetinio saugumo valdymo sistema. 2014 m. redakcijos Įstatyme numatyta, kad kibernetinio saugumo politiką formuoja ir jos įgyvendinimą koordinuoja Krašto apsaugos ministerija, politikos formavime dalyvauja ir politiką įgyvendina Vidaus reikalų ministerija, Nacionalinis

[101] Programa oficialiai pripažinta netekusia galios Lietuvos Respublikos Vyriausybės 2019 m. liepos 3 d. nutarimo Nr. 709 "Dėl Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano patvirtinimo" 2 punktu. Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/faeb5eb4a6c811e9aab6d8dd69c6da66?jfwid=dg8d31595

[102] Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595

[103] Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/15e540727ac211e89188e16a6495e98c

kibernetinio saugumo centras[104], Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija ir Policijos departamentas, kibernetinio saugumo būklę analizuoja ir siūlymus dėl jos gerinimo teikia Kibernetinio saugumo taryba. 2018 m. redakcijos Įstatyme kibernetinio saugumo politikos strateginių tikslų ir prioritetų nustatymo įgaliojimai suteikti Vyriausybei, Krašto apsaugos ministerija išliko kibernetinio saugumo politiką formuojančia ir jos įgyvendinimą koordinuojančia institucija. Išplėstos Nacionalinio kibernetinio saugumo centro funkcijos (numatyta pareiga informuoti visuomenę apie pavienius incidentus arba reikalauti, kad tai padarytų kibernetinio saugumo subjektas, taip pat nustatyta teisė reikalauti, kad kibernetinio saugumo subjektai teiktų informaciją, reikalingą jų ryšių ir informacinių sistemų kibernetiniam saugumui įvertinti ir duoti privalomus nurodymus pašalinti kibernetinio saugumo reikalavimų įgyvendinimo trūkumus), į kibernetinio saugumo politikos įgyvendinimą įtrauktos „kitos institucijos, kurių funkcijos susijusios su kibernetiniu saugumu“ (4 straipsnio 3 dalis).

Pažymėtina, kad 2018 m. redakcijos Įstatyme išplėstas kibernetinio saugumo principų sąrašas. 2014 m. redakcijos Įstatymo 3 straipsnio 1 dalyje numatyti trys principai: *kibernetinės erdvės nediskriminavimo, kibernetinio saugumo proporcingumo* ir *viešojo intereso viršenybės.* Šiuo metu galiojančio Įstatymo 3 straipsnio 1 dalyje įtvirtintas kibernetinio saugumo principų sąrašas papildytas *kibernetinio saugumo rizikos valdymo* principu (taikomos priemonės turi užtikrinti reguliariai įvertinamos rizikos suvaldymą), *standartizacijos ir technologinio neutralumo* principu (nereikalaujama suteikti pirmenybę konkrečios rūšies technologijai) ir *subsidiarumo* principu (kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos veiksmų imasi tik tada, kai ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinio saugumo negali užtikrinti šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai).

2018–2023 m. kibernetinio saugumo strategijoje nurodoma, kad ji parengta atsižvelgiant į aplinkos analizę, atliktų tyrimų duomenis, viešojo ir privataus sektorių atstovų pasiūlymus. Dokumente nustatyti penki **tikslai** ir kiekvienam jų įgyvendinti numatyti **uždaviniai** (15)**.** Aptarsiu juos plačiau.

1. *Valstybės kibernetinio saugumo stiprinimas ir kibernetinių gynybos pajėgumų plėtra.* Pažymima, kad Lietuva nuolat susiduria su pačiais įvairiausiais kibernetiniais incidentais, skirtais valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai pažeisti, prognozuojama, kad jų skaičius ateityje ženkliai nemažės. Be to, nors pavieniai įvairių saugumo sričių rizikos vertinimo procesai pasiekė brandą, saugumo rizikos vertinimo kultūra, kibernetinio saugumo rizikos vertinimas tebėra fragmentiškas. Dėl šių priežasčių būtinas integralios kibernetinio saugumo vadybos sistemos sukūrimas, kompetencijų kibernetinio saugumo srityje tobulinimas.

[104] Pagrindinė Lietuvos kibernetinio saugumo institucija, atsakinga už vieningą kibernetinių incidentų valdymą, kibernetinio saugumo reikalavimų įgyvendinimo stebėseną ir kontrolę. Centras veiklą vykdo nuo 2015 m., įkurtas pertvarkius Ryšių ir informacinių sistemų tarnybą prie Krašto apsaugos ministerijos.

Tikslo įgyvendinimui numatyti šie uždaviniai: 1) sisteminio požiūrio į kibernetinį saugumą ir prevencinę veiklą kūrimas (numatoma suformuoti kibernetinio saugumo rizikos žemėlapį, įtraukti valstybės ir savivaldybių institucijas, įstaigas ir įmones į kibernetinio saugumo būklės tyrimus, informuoti visuomenę apie kibernetinio saugumo būklę); 2) kibernetinio saugumo politikos formavimo ir įgyvendinimo efektyvumo didinimas, administracinės naštos kibernetinio saugumo subjektams mažinimas (numatoma parengti standartizuotus, bet diferencijuotus kibernetinio saugumo reikalavimus, stiprinti bendradarbiavimą); 3) nacionalinių kibernetinio saugumo pratybų skatinimas, dalyvavimas tarptautinėse pratybose; 4) valstybės kibernetinės gynybos pajėgumų plėtra (karinių ir civilinių pajėgumų sąveika, pagalba kitoms valstybės ir savivaldybių institucijoms ir įstaigoms).

Nurodyto tikslo reikšmingumas neginčytinas, tačiau jo įgyvendinimui pasirinktos priemonės, autoriaus manymu, pernelyg abstrakčios, nepamatuojamos ir jų galutinis rezultatas neaiškus. Be to, tokių priemonių kaip „kitos“ (įgyvendinant antrąjį uždavinį numatyta taikyti „*kitas kibernetinio saugumo politikos formavimo ir įgyvendinimo plėtojimo priemones*“) strategijoje neturėtų būti.

2. *Nusikalstamų veikų kibernetinėje erdvėje prevencija, užkardymas ir tyrimas.* Skaičiai kalba patys už save: strategijos rengimo metu, 2017 m. Nusikalstamų veikų žinybinio registro duomenimis registruotos 594 tokios veikos (2016 m. – 336). Elektroniniai nusikaltimai peržengia valstybių sienas, todėl efektyvi kova su jais be tarptautinio bendradarbiavimo neįmanoma.

Strategijoje numatyti du šio tikslo įgyvendinimo uždaviniai: 1) valstybės gebėjimų kovojant su nusikalstamomis veikomis elektroninėje erdvėje plėtojimas (teisėkūra, teisėsaugos institucijose dirbančių specialistų kvalifikacijos tobulinimas, pažangių technikos bei veiklos metodų diegimas); 2) nusikalstamų veikų kibernetinėje erdvėje prevencija ir kontrolė (visuomenės švietimas, tarptautinio bendradarbiavimo stiprinimas). Ypač teigiamai vertintinas strategijoje numatytas bendradarbiavimas su mokslo ir studijų institucijomis, privataus sektoriaus atstovais, tačiau norėtųsi konkretesnių bendradarbiavimo skatinimo priemonių nustatymo.

3. *Kibernetinio saugumo kultūros ir inovacijų plėtra.* Strategijoje atkreipiamas dėmesys į tai, kad Europos valstybių privataus sektoriaus atstovai didina investicijas, skirtas darbuotojų mokymams informacinių technologijų srityje, tačiau Lietuvoje šis rodiklis tik truputį viršija 10 proc. (rodiklio vidurkis Europoje – 21 proc.)[105]. Be to, trūksta reguliarių ir naujausiomis tendencijomis pagrįstų viešojo ir privataus sektorių darbuotojų mokymo kibernetinio saugumo srityje, specialių mokymo programų priešmokyklinio, pradinio, vidurinio ugdymo moksleiviams, pedagogams, esamų kibernetinio saugumo specialistų skaičius nepakankamas. Kitas svarbus aspektas – parama privataus sektoriaus atstovams, kuriantiems ir diegiantiems kibernetinio saugumo srities inovacijas, mokslininkų skatinimas įsitraukti į inovacijų kūrimo ir diegimo procesus, taip pat ir tarptautiniu lygmeniu.

[105] IBM X-Force Threat Intelligence Index 2018. Prieiga internetu: www.justincolman.com/wp-content/uploads/2019/03/Threat-Intelligence-2018-IBM-X-Force.pdf

Uždaviniai trys: 1) mokslinių tyrimų ir didelę pridėtinę vertę kuriančių veiklų kibernetinio saugumo srityje plėtra; 2) kūrybiškumo, pažangių gebėjimų ir rinkos poreikius atitinkančių kibernetinio saugumo įgūdžių ir kvalifikacijos ugdymas (numatoma sukurti atitinkamų kompetencijų modelį, plėtoti mokymų, akreditavimo ir sertifikavimo sistemas, orientuotas į darbo rinkos poreikius, talentų ugdymą); 3) viešojo ir privataus sektorių bei mokslo ir studijų institucijų bendradarbiavimo, kuriant kibernetinio saugumo srities inovacijas, skatinimas.

4. *Glaudaus viešojo ir privataus sektorių bendradarbiavimo stiprinimas.* Tokio tikslo numatymas vertintinas teigiamai. Viešojo ir privataus sektorių bendradarbiavimas kibernetinio saugumo srityje nėra ta sritis, kurioje puikiais rezultatais galėtų pasigirti daugelis kibernetinio saugumo strategijas įgyvendinančių valstybių. Strategijoje nurodoma, kad bendradarbiavimo poreikis abipusis, viešojo sektoriaus atstovams per sunku vieniems kovoti su pavojingais ar didelės reikšmės kibernetiniais incidentais, o privataus sektoriaus atstovai neretai nepajėgia suvaldyti kibernetinių incidentų, peržengiančių organizacijos ribas. Viešojo ir privataus sektorių bendradarbiavimui įgyvendinti įdiegtas Kibernetinio saugumo informacinis tinklas[106] reikalauja papildomų priemonių, užtikrinančių efektyvų ir abipusį pasitikėjimą skatinantį tinklo narių bendravimą, diegimo.

Tikslas įgyvendinamas: 1) gerinant viešojo ir privataus sektorių bendradarbiavimo koordinavimą (atkreiptinas dėmesys į ankstyvojo perspėjimo sistemos plėtojimą, naujų komunikacijos metodų ir procesų kūrimą), 2) didinant viešojo bei mažų ir vidutinių privataus sektorių atstovų kibernetinio saugumo brandą (tai pasireikš per skatinimą tikrintis kibernetinio saugumo būklę ir taisyti aptiktas kibernetinio saugumo spragas) ir 3) kuriant atsakingą viešojo ir privataus sektorių saugumo spragų atskleidimo praktiką.

5. *Tarptautinio bendradarbiavimo stiprinimas, tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymas.* Tikslas pamatuotas, siekiama aktyviai dalyvauti tarptautinės kibernetinės politikos kūrimo procese tiek dvišaliu, tiek daugiašaliu lygmeniu. Tikslo įgyvendinimui numatyti uždaviniai taip pat pakankamai standartiniai: 1) plėtoti tarptautinį, tarpvalstybinį ir Baltijos regiono šalių bendradarbiavimą; 2) stiprinti tarptautinius kibernetinio saugumo pajėgumus ir gebėjimus (numatoma inicijuoti Nuolatinio struktūrizuoto bendradarbiavimo projektą ir jam vadovauti); 3) dialogo su Jungtinėmis Amerikos Valstijomis kibernetinės gynybos srityje plėtra.

Lietuvos Respublikos Vyriausybės 2019 m. liepos 3 d. nutarimu Nr. 709 "Dėl Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano patvirtinimo" patvirtintas Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, kurio įgyvendinimą koordinuoti pavesta Krašto apsaugos ministerijai. Pažymėtina, kad nevyriausybinės organizacijos, suinteresuoti viešojo ir privataus sektorių atstovai, Lietuvos mokslo ir studijų

[106] Tinklas apjungia Nacionalinio kibernetinio saugumo centro teikiamus resursus ir paslaugas vienoje erdvėje, siekiant užtikrinti efektyvų kibernetinio saugumo informacijos dalinimąsi tarp visų kibernetinio saugumo subjektų. Plačiau: https://www.nksc.lt/kontaktai.html

institucijos nėra strategijos vykdytojos, tačiau gali prisidėti prie jos vykdymo, tikslų ir uždavinių siekimo.

Kasmet, ne vėliau kaip iki einamųjų metų sausio 15 d., Nacionalinis kibernetinio saugumo centras pateikia informaciją apie strategijos įgyvendinimo eigą, veiksmingumą ir tai pagrindžiančius duomenis. Kartu su šia informacija gali būti pateikti siūlymai dėl strategijos tikslinimo. Be to, 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 strategijoje numatytas priemones. Krašto apsaugos ministerija kasmet iki kovo 1 d. apibendrina gautą informaciją apie strategijos įgyvendinimo eigą, veiksmingumą ir susistemintus duomenis apie strategijos metinį įgyvendinimą pristato Kibernetinio saugumo tarybai ir pateikia Vyriausybei.

Vadovaujantis apibendrinta ataskaita už 2020 m.[107], dalies uždavinių vykdymą sustabdė ar apribojo COVID-19 pandemijos sukelti ribojimai. Daugiausia pastangų ir lėšų skirta kibernetinio saugumo stiprinimui ir kibernetinių gynybos pajėgumų plėtrai. Sėkmingai diegtos ir įgyvendintos šios priemonės: tobulinti Kibernetinio saugumo informacinio tinklo pajėgumai, surengtos kasmetinės nacionalinės kibernetinio saugumo pratybos „Kibernetinis skydas 2020“, tęsiamas nuolatinio struktūrizuoto bendradarbiavimo projekto „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“ įgyvendinimas, pradėtas įgyvendinti Europos Sąjungos struktūrinių fondų finansuojamas projektas „Kompleksiniai kibernetinės saugos mokymai valstybės ir savivaldybių institucijų ir įstaigų dirbantiesiems“, sukurta *Map of Public Internet* sistema, leidžianti Nacionaliniam kibernetinio saugumo centrui realiu laiku stebėti Lietuvos kibernetinės erdvės ekosistemos anomalijas ir grėsmes, tinkamai į jas reaguoti. Taip pat nemažai nuveikta mokymo, švietimo ir visuomenės informavimo apie kibernetines grėsmes srityje.

Ataskaitoje taip pat pateikta detali informacija apie atskirų strategijos vykdytojų veiksmus, įgyvendinant strategiją ir pasiektus rezultatus.

Konkretūs siūlymai 2018–2023 m. nacionalinės kibernetinio saugumo strategijos tobulinimui bus pateikti kitame šio darbo skyriuje.

[107] Prieiga internetu: https://www.nksc.lt/aktualu.html

4. LIETUVOS KIBERNETINIO SAUGUMO STRATEGIJOS MODELIS

4.1 Modeliavimo metodologija

Nacionalinių kibernetinio saugumo strategijų, nustatančių esminius kibernetinio saugumo užtikrinimo principus, tikslus, prioritetus ir detalius kibernetinio saugumo priemonių įgyvendinimo planus, poreikis išliks dar ilgai. Kibernetinė erdvė yra dinamiška, grėsmių jai skaičius nuolat auga, kibernetinės grėsmės tampa vis sudėtingesnėmis, todėl visiškai natūralu, kad kibernetinio saugumo politika tampa nacionalinės politikos prioritetu. Nacionalinė kibernetinio saugumo strategija yra pagrindinis „įrankis“ nustatantis rekomendacijas, į kurias reikėtų atsižvelgti, užkertant kelią kibernetinėms grėsmėms.

Tinkamos, realiai įgyvendinamos kibernetinio saugumo strategijos, kurioje būtų numatytos aktualiausios tam tikram laikotarpiui grėsmės ir pasirinktos efektyviausios ir inovatyviausios kovos su grėsmėmis priemonės, parengimas – sudėtingas procesas. Rekomendacijas tokio pobūdžio dokumentų rengimui teikia tiek tarptautinės organizacijos, tiek įvairių valstybių mokslininkai. Lietuvos mokslininkai 2015–2017 m. rengė ir 2017 m. pateikė Lietuvos kibernetinio saugumo strategijos modelį[108]. Modelis parengtas išanalizavus Europos Sąjungos ir NATO kibernetinio saugumo strategijų normas, įvairių užsienio valstybių patirtį, diegiant kibernetinio saugumo priemones. Šis modelis numato gaires nacionalinės kibernetinio saugumo strategijos parengimui, pateikia lengvai suprantamas ir nesunkiai įgyvendinamas rekomendacijas. Paminėsiu esmines iš jų: strategijos kūrimas ne ilgesniam, nei penkerių metų laikotarpiui; atsakomybės už strategijos rengimą ir priežiūrą suteikimas vienai institucijai; strategijos ir joje numatytų priemonių įgyvendinimo plano atskyrimas; reguliari strategijoje numatytų priemonių įgyvendinimo peržiūra; aiški terminologija.

Modelyje nemažai dėmesio skiriama kibernetinio saugumo principų aptarimui. Įdomu tai, kad išskiriamas ir aptariamas *asmeninės atsakomybės* principas, reiškiantis, kad kiekvienas kibernetinio saugumo dalyvis turi būti atsakingas už kibernetinio saugumo palaikymą. Tai itin svarbu, nes nemaža dalis kibernetinių incidentų įvyksta dėl nepakankamo informacines technologijas naudojančio asmens atsargumo, apdairumo ar net sąmoningo esminių saugaus elgesio principų ignoravimo. Nepaisant to, šis principas nėra įtrauktas į šiuo metu galiojančio Kibernetinio saugumo įstatymo 3 straipsnyje išvardytus kibernetinio saugumo principus. Modelį kūrę mokslininkai 2017 m. parengė rekomendacijas Kibernetinio saugumo įstatymui[109], kuriose, akcentuodami asmeninės atsakomybės

[108] Autorių kolektyvas: dr. Darius Štitilis, dr. Paulius Pakutinskas, dr. Marius Laurinaitis, Inga Malinauskaitė–van de Castel. Lietuvos kibernetinio saugumo strategijos modelis. Mykolo Romerio universitetas, Vilnius, 2017.

[109] Autorių kolektyvas: dr. Darius Štitilis, dr. Paulius Pakutinskas, dr. Marius Laurinaitis, Inga Malinauskaitė–van de Castel. Rekomendacijos Lietuvos Respublikos kibernetinio saugumo įstatymui. Mykolo Romerio universitetas, Vilnius, 2017. P. 6.

principo įtraukimo į įstatyme įtvirtintą principų sistemą, nurodė, kad „kibernetinis neraštingumas gali skatinti kibernetinius incidentus“.

Autoriaus siūlomo kibernetinio saugumo strategijos modelio metodologija remiasi analizei pasirinktų užsienio valstybių – Jungtinių Amerikos Valstijų, Jungtinės Karalystės, Pietų Korėjos, Australijos, Vokietijos, Prancūzijos, Ispanijos gerąja patirtimi, kuriant kibernetinio saugumo strategijas ir įgyvendinant jose numatytas priemones. Dalies analizuotų valstybių patirtimi nesivadovauta tiek dėl strategijose numatytų priemonių abstraktumo, tiek dėl informacijos apie strategijų įgyvendinimą neprieinamumo (Kinijos atvejis).

Modeliavimas buvo vykdomas remiantis šiais metodais:

1) *dokumentų analizės:* analizuoti tiek pasirinktų užsienio valstybių kibernetinio saugumo strategijų tekstai, jų lydimieji dokumentai (priemonių planai), tiek ataskaitos apie strategijų įgyvendinimą. Taip pat nemažai dėmesio skirta Europos Sąjungos kibernetinio saugumo agentūros 2016 m. tyrimo ir BSA Programinės įrangos aljanso 2015 m. tyrimo dėl nacionalinių kibernetinio saugumo strategijų įgyvendinimo rezultatų apžvalgai. Detaliai išanalizuoti Lietuvos kibernetinio saugumo klausimus reglamentuojantys teisės aktai, pradedant Lietuvos Respublikos Vyriausybės 2001 m. gruodžio 22 d. nutarimu Nr. 1625 patvirtinta Informacijos technologijų saugos valstybine strategija ir jos įgyvendinimo planu, baigiant 2018–2023 m. Nacionaline kibernetinio saugumo strategija ir kasmet Nacionalinio kibernetinio saugumo centro teikiama informacija apie strategijos įgyvendinimo eigą ir veiksmingumą;

2) *apibendrinimo:* didžiausias dėmesys buvo skiriamas šiems kibernetinio saugumo strategijose numatytiems uždaviniams ir jų įgyvendinimui skirtoms priemonėms: privataus ir viešojo sektoriaus bendradarbiavimo įgyvendinimui, visuomenės švietimui kibernetinio saugumo klausimais, ypatingos svarbos informacinės infrastruktūros apsaugai, elektroninių nusikaltimų prevencijai ir jų latentiškumo mažinimui bei tarptautiniam bendradarbiavimui;

3) *lyginimo:* atsižvelgta į skirtingą valstybių patirtį, kuriant ir diegiant kibernetinio saugumo strategijas, ženkliai besiskiriančias finansines galimybes įdiegti inovatyviausias kibernetinio saugumo priemones, taip pat įvertinta, ar valstybių kuriamos strategijos vertintinos kaip tęstinės (ne tik parengtų dokumentų skaičių, periodiškumą, bet ir numatytų įgyvendinti priemonių tęstinumą);

4) *kiti metodai:* loginės analizės, sisteminės analizės, dedukcijos, atvejo analizės metodai.

Autoriaus siūlomas kibernetinio saugumo strategijos modelis apima tris sritis:

1. Strategijos rengimo proceso. Manytina, kad rengiant naują Lietuvos nacionalinę kibernetinio saugumo strategiją būtina ne tik atlikti aplinkos analizę, atsižvelgti į atliktų tyrimų duomenis, viešojo ir

privataus sektorių atstovų pasiūlymus[110], bet ir detalizuoti, kokių būtent tyrimų duomenys reikšmingi naujai strategijai, kas ir kokius siūlymus pateikė, dėl kokių priežasčių į tam tikrus siūlymus neatsižvelgta. Be to, būtų tikslinga išskirti akademinės bendruomenės teikiamus siūlymus ir rekomendacijas. Rengiant kibernetinio saugumo strategiją būtina ir detali ankstesnės strategijos įgyvendinimo rezultatų analizė, kitaip atitinkamų priemonių tęstinumas neįsivaizduojamas.

2. Atitinkamų prioritetinių priemonių įtraukimo į kibernetinio saugumo strategijos priemonių įgyvendinimo planą. Lietuvos mokslininkai 2017 m. pateiktame kibernetinio saugumo strategijos modelyje išskyrė 7 pagrindines veiksmų sritis, kurios turėtų būti įtrauktos į valstybės nacionalinę kibernetinio saugumo strategiją: 1) ypatingos svarbos informacinės infrastruktūros apsauga; 2) valstybės informacinių išteklių apsauga; 3) privataus ir viešojo sektoriaus bendradarbiavimas; 4) institucinės sistemos išgryninimas; 5) kibernetinės kultūros vystymas; 6) tarptautinis bendradarbiavimas; 7) teisinės aplinkos vystymas. Šios sritys aktualumo neprarado ir autoriaus siūlomame modelyje jos bus tik iš dalies pakoreguotos.

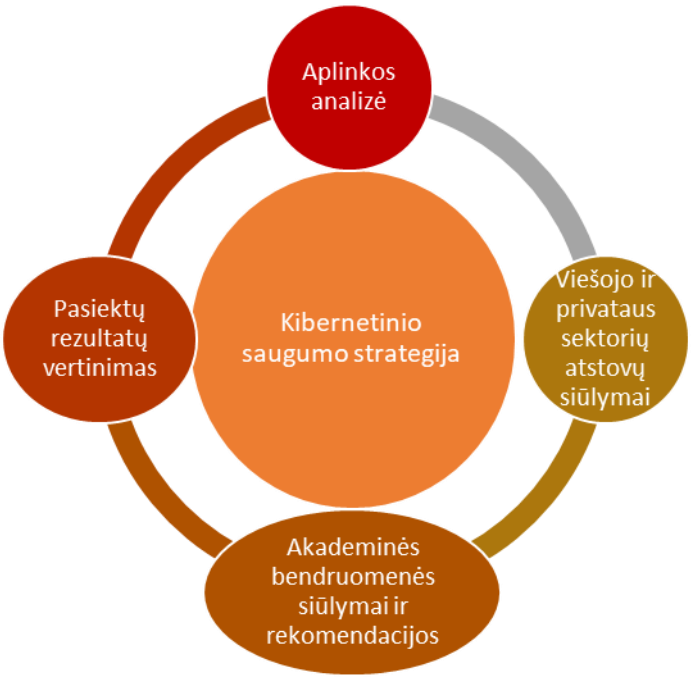
3. Strategijoje numatytų priemonių įgyvendinimo vertinimas. Autoriaus manymu, šiuo metu galiojančioje kibernetinio saugumo strategijoje numatytas atsiskaitymo už atitinkamų priemonių įgyvendinimo rezultatus mechanizmas nepakankamai detaliai reglamentuotas.

Svarbu pažymėti ir tai, kad nors galiojančioje strategijoje numatyta galimybė visiems suinteresuotiems subjektams teikti siūlymus dėl strategijos nuostatų atnaujinimo, nenumatytas gautų siūlymų nagrinėjimo ir sprendimo dėl jų priėmimo mechanizmas.

4.2 Modelio rezultatų analizė

1. Strategijos rengimo procesas. Modelyje siūloma išplėsti rengiant strategiją analizuotinų duomenų sąrašą, taip pat subjektų, teikiančių siūlymus dėl strategijos ir į jos įgyvendinimo priemonių planą įtrauktinų priemonių, ratą. Ypatingą dėmesį skirti akademinės bendruomenės siūlymams ir rekomendacijoms. Be to, siekiant užtikinti kibernetinio saugumo įgyvendinimo priemonių tęstinumą, būtina detali ankstesnėje strategijoje numatytų priemonių įgyvendinimo rezultatų analizė, įvertinant, dėl kokių priežasčių atitinkamos priemonės nebuvo įgyvendintos ir ar jos vis dar aktualios.

[110] Galiojančioje Lietuvos kibernetinio saugumo strategijoje nurodyta, kad ji parengta „atsižvelgiant į aplinkos analizę, atliktų tyrimų duomenis, viešojo ir privataus atstovų sektorių pasiūlymus“.



Pavyzdys Nr. 6

2. Prioritetinės į strategiją įtrauktinų veiksmų sritys[111]:

1) *Ypatingos svarbos informacinės infrastruktūros apsauga* ir 2) *valstybės informacinių išteklių apsauga*. Manytina, kad šios sritys, atsižvelgiant į jų įgyvendinimui numatytų priemonių panašumą, galėtų būti apjungtos. Galiojančioje kibernetinio saugumo strategijoje šios veiksmų sritys nėra suformuluotos kaip atskiri tikslai, o jų įgyvendinimui skirtos priemonės pateiktos per kibernetinio saugumo ir kibernetinės gynybos pajėgumų stiprinimą. Pažangios ir iš dalies jau įgyvendintos priemonės būtų jau sukurta *Map of Public Internet* sistema, leidžianti Nacionaliniam kibernetinio saugumo centrui realiu laiku stebėti Lietuvos kibernetinės erdvės ekosistemos anomalijas ir grėsmes, tinkamai reaguoti į jas, taip pat diegiant nacionalinį integruotą krizių valdymo mechanizmą. Šios sistemos pajėgumų tobulinimas turėtų būti numatytas naujoje strategijoje kaip pažangi tęstinė priemonė.

3) *Privataus ir viešojo sektoriaus bendradarbiavimas.* Džiugu, kad bendradarbiavimo stiprinimas numatytas kaip vienas iš galiojančios strategijos tikslų ir kad puikiai suvokiama abipusė tokio bendradarbiavimo nauda, tačiau pastebėtina, kad bendradarbiavimo stiprinimui numatytoms priemonėms trūksta konkretumo. Čia galėtų pagelbėti geroji kitų valstybių, kuriose itin išvystyta viešojo ir privataus sektorių bendradarbiavimo sistema (Jungtinės Amerikos Valstijos, Vokietija, Australija), patirtis. Svarstytinas esmines kibernetinio saugumo problemas svarstančios ir siūlymus dėl jos teikiančios komisijos (darbo grupės) sukūrimas. Į komisijos (darbo grupės) sudėtį, be strategijoje

[111] Autorius rėmėsi Lietuvos mokslininkų 2017 m. pateiktame Lietuvos kibernetinio saugumo strategijos modelyje išskirtomis pagrindinėmis veiksmų sritimis, įtrauktinomis į strategiją ir pateikė savo siūlymus dėl strategijos pildymo naujomis konkrečiomis priemonėmis.

numatytas priemones vykdančių subjektų – viešojo sektoriaus institucijų atstovų, būtų įtraukti privataus sektoriaus atstovai, taip pat akademinės bendruomenės nariai. Komisijos sprendimai neturėtų privalomosios galios, būtų rekomendaciniai, tačiau, prieš priimant atitinkamus sprendimus kibernetinio saugumo srityje, žinoti visų suinteresuotų subjektų nuomones būtų itin vertinga. Svarbu ir tai, kad tokios bendradarbiavimą stiprinančios priemonės įtraukimas į strategiją nepareikalautų nei itin didelių finansinių, nei laiko sąnaudų (komisijos posėdžiai galėtų būti organizuojami kas pusmetį ar pagal poreikį).

4) *Institucinės sistemos išgryninimas.* Kaip vienas iš šios veiksmų srities prioritetų Modelyje numatomas pranešimų apie teisės pažeidimus elektroninėje erdvėje veikimo užtikrinimas. Įgyvendinant šios srities veiksmus galiojančioje strategijoje, autoriaus siūlymu, būtų svarstytinas platformos, kurioje asmenys galėtų anonimiškai pasikonsultuoti dėl patirtų kibernetinių incidentų ar veikų, galinčių būti kvalifikuotomis kaip elektroniniai nusikaltimai, gauti kvalifikuotų patarimų, įdiegimas. Pavyzdžiu galėtų būti Prancūzija, įdiegusi platformą, kurioje nukentėjusiems nuo veikų, kurios potencialiai gali būti pripažintos elektroniniais nusikaltimais, anonimiškai (jei asmuo to pageidauja) teikiamos konsultacijos, taip pat reali techninė pagalba (duomenų vagysčių, įsilaužimų, pakenkimo programinei įrangai atvejais). Dar vienu gerosios praktikos pavyzdžiu galėtų būti laikoma Jungtinėje Karalystėje veikianti 24/7 platforma (teikia konsultacijas, bet ne fizinę techninę pagalbą). Svarbu ir tai, kad tokio pobūdžio platformos padėtų sumažinti elektroninių nusikaltimų latentiškumą, nes viena iš priežasčių, dėl kurių neinformuojama apie elektroninius nusikaltimus, yra asmens nesupratimas, su kuo jis susidūrė – informacinių technologijų gedimu, pokštu, ar piktavališkais veiksmais. Priklausomai nuo biudžeto galimybių, steigiama platforma galėtų veikti ne visą parą, o joje konsultacijas teiktų (savanorystės pagrindu ar praktiką atlikdami) studentai.

5) *Kibernetinės kultūros vystymas* (švietimas, visuomenės suvokimo apie kibernetinio saugumo grėsmes ir saugaus elgesio elektroninėje erdvėje principus didinimas, įvairūs mokymai). Pažymėtina, kad galiojančioje strategijoje tam numatyta nemažai priemonių ir jau pasiekti neblogi rezultatai, tačiau, autoriaus pastebėjimu, planuojant švietimą kibernetinio saugumo srityje, diegiant ir tobulinant įvairias mokymo programas, pasigendama dėmesio visoms visuomenės grupės, ypač tokioms kaip garbaus amžiaus asmenys. Šiuo atveju vertėtų įvertinti gerąją Vokietijos praktiką ir ieškoti būdų būtiniausias žinias kibernetinio saugumo srityje suteikti ir senjorams, kurių aktyvumas, naudojantis informacinėmis technologijomis palaipsniui didėja. Švietimo priemonės galėtų būti pačios paprasčiausios – esminės informacijos patalpinimas į atitinkamą platformą mokomosios medžiagos ir interaktyvaus testo pavidalu. Manyčiau, kad šiuo atveju pagelbėtų bendradarbiavimas su bibliotekomis, kuriose reguliariai organizuojami užsiėmimai senjorams, taip pat seniūnijos, skatinančios ir palaikančios senjorų klubų ir susibūrimų veiklą.

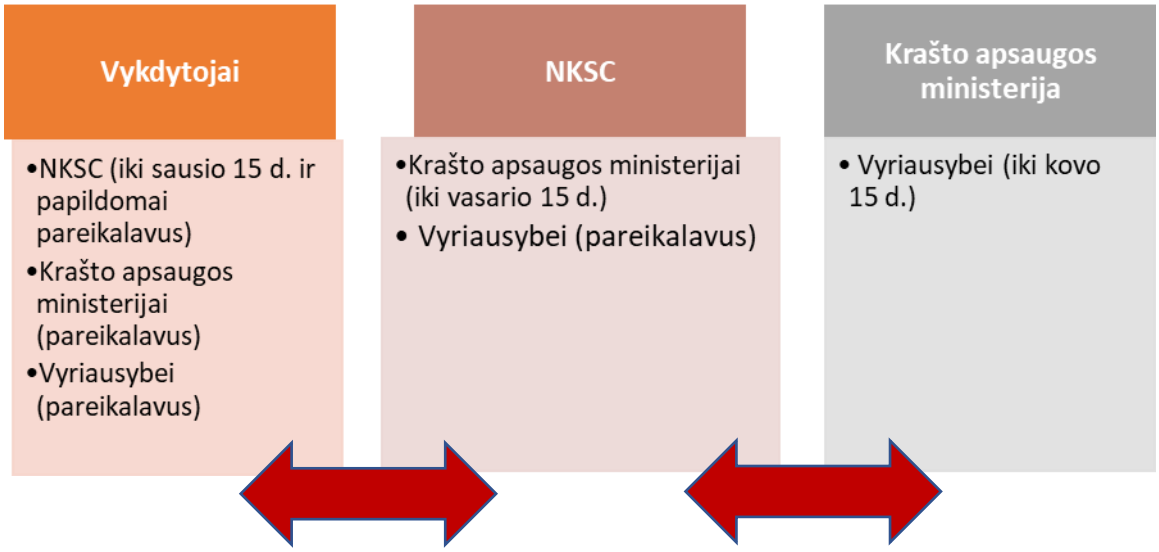
6) *Tarptautinis bendradarbiavimas.* Įgyvendinant šios srities priemones, esminių pastabų ar pasiūlymų galiojančiai kibernetinio saugumo strategijai nebūtų.

7) *Teisinės aplinkos vystymas* (ypač akcentuotinas skirtinguose teisės aktuose vartojamų sąvokų suvienodinimas). Strategijoje pasisakyta apie atitinkamus teisėkūros aspektus, tik autoriaus manymu, vertėtų pasvarstyti ir apie *asmeninės atsakomybės* principo įtraukimą į kibernetinio saugumo principų sistemą, nustatytą Kibernetinio saugumo įstatymo 3 straipsnyje. Be to, šio principo reikšmė ir svarba turėtų būti akcentuota visų organizuojamų mokymų kibernetinio saugumo klausimais metu.

3. Strategijoje numatytų priemonių įgyvendinimo vertinimas. Galiojančioje strategijoje nurodyta, kad jos vykdytojai kasmet iki sausio 15 d. Nacionaliniam kibernetinio saugumo centrui pateikia informaciją apie strategijoje numatytų priemonių įgyvendinimo eigą bei veiksmingumą, taip pat gali teikti siūlymus dėl strategijos ir joje numatytų įgyvendinti priemonių tikslinimo. Nacionalinis kibernetinio saugumo centras susistemina gautą informaciją ir kasmet iki vasario 1 d. pateikia ją Krašto apsaugos ministerijai, kartu nurodydamas problemines sritis, trukdančias tinkamai įgyvendinti strategiją. Krašto apsaugos ministerijai suteikiamas mėnuo (iki einamųjų metų kovo 1 d.) gautos informacijos apibendrinimui ir jos pateikimui Vyriausybei.

Manytina, kad tokia ataskaitos schema iš esmės yra tinkama, tačiau būtina jos detalizacija. Strategijos vykdytojai turėtų detalizuoti priežastis, dėl kurių atitinkamos priemonės nebuvo įgyvendintos ir tokiomis priežastimis neturėtų būti pripažinti abstraktūs paaiškinimai, tokie kaip „laiko ar žmogiškųjų išteklių trūkumas“. Taip pat manytina, kad Nacionalinis kibernetinio saugumo centras turėtų neapsiriboti vien papildomos informacijos pareikalavimu, bet galėtų vertinti atitinkamos priemonės neįgyvendinimą ar tik dalinį įgyvendinimą kaip patenkinamą arba nepatenkinamą, o tokiai analizei, atsižvelgiant į galimybę reikalauti papildomos informacijos, o ją gavus – analizuoti ir vertinti, dviejų savaičių terminas nepakankamas.

Pavyzdys Nr. 7. Autoriaus siūloma ataskaitų teikimo schema



IŠVADOS

1. Suvokimas, kad efektyvių kibernetinio saugumo užtikrinimo priemonių įgyvendinimas, elektroninių nusikaltimų prevencija vien nacionaliniu lygmeniu neįmanomas, akivaizdus visų analizuotų valstybių nacionalinėse kibernetinio saugumo strategijose. Iš esmės skiriasi tik tai, ar valstybės siekia lyderystės formuojant tarptautinę kibernetinio saugumo politiką (Jungtinės Amerikos Valstijos, Kinija, Australija), ar apsiriboja aktyviu dalyvavimu tarptautinio pobūdžio priemonių įgyvendinime.

Be to, visos analizei pasirinktos valstybės įgyvendinamose kibernetinio saugumo strategijose yra numačiusios priemones kritinės svarbos informacinių infrastruktūrų apsaugai. Techninių saugos priemonių diegimas orientuojamas į rinkos palaikymą (parama saugumo standartus atitinkančius produktus kuriančioms ir diegiančioms įmonėms, standartizacijos procesų tobulinimas ir kt.) ir elektroninių nusikaltimų prevenciją. Itin skatintinu pavyzdžiu laikytinas specialių platformų, kuriose, susidūrus su nepageidautinais piktaviliškais veiksmais elektroninėje erdvėje, galima gauti kvalifikuotą konsultaciją (pareiškėjui pageidaujant – anonimiškai), ar net realią techninę pagalbą.

2. Visuomenės švietimo kibernetinio saugumo klausimais, kvalifikuotų kibernetinio saugumo specialistų rengimo svarba taip pat pripažįstama visų nagrinėtų valstybių kibernetinio saugumo strategijose, tačiau numatytos priemonės skiriasi. Vokietija ir Portugalija orientuojasi į visų visuomenės grupių švietimą, neišskiriant nei darželinukų, nei garbaus amžiaus asmenų. Prancūzija, Jungtinė Karalystė švietimą orientuoja į aukštąjį mokslą, doktorantus, informacinių technologijų studentus. Be to, visos analizuotos valstybės į strategijas yra įtraukusios bendradarbiavimo su akademine bendruomene priemonių, skiriasi tik jų įgyvendinimo intensyvumas.

3. Valstybių požiūriai į viešojo ir privataus sektorių bendradarbiavimą įgyvendinant kibernetinio saugumo priemones ir sprendžiant kibernetinio saugumo problemas skiriasi. Visose analizuotose kibernetinio saugumo strategijose privataus sektoriaus įtraukimas nurodomas kaip strateginis tikslas ar kaip kurio nors kito tikslo įgyvendinimo uždavinys, tačiau realių ir veiksmingų priemonių, užtikrinančių efektyvų privataus sektoriaus įsitraukimą, trūksta. Gerosios praktikos pavyzdžiu laikytinos Jungtinės Amerikos Valstijos ir Vokietija, kuriose jokie esminiai sprendimai, susiję su kibernetinio saugumo problemomis, nepriimami be privataus sektoriaus subjektų dalyvavimo.

4. Lietuvos 2018–2023 m. nacionalinėje kibernetinio saugumo strategijoje numatyti tikslai ir prioritetinės veiksmų kibernetinio saugumo srityje įgyvendinimo kryptys iš esmės nesiskiria nuo kitų valstybių strategijose numatytųjų, įtvirtinta aiški strategiją įgyvendinančių subjektų sistema. Numatytos įgyvendinti priemonės galėtų būti papildytos pasirinktų valstybių analizuotų strategijų gerosios praktikos pavyzdžiais, be to, tobulintina ataskaitų už strategijoje numatytų priemonių įgyvendinimą teikimo ir vertinimo sistema.

PASIŪLYMAI

1. Atsižvelgiant į tai, kad nemaža dalis kibernetinių incidentų kyla dėl neatsargių informacines technologijas naudojančio asmens veiksmų ar sąmoningo saugumo principų nesilaikymo, taip pat į tai, kad net pačios tobuliausios technologijos negali apsaugoti nuo žmogiškosios klaidos, siūlytina *asmeninės atsakomybės* principą įtraukti į kibernetinio saugumo principų sistemą, nustatytą Lietuvos Respublikos kibernetinio saugumo įstatymo 3 straipsnyje.

2. Į Lietuvos 2018–2023 m. nacionalinėje kibernetinio saugumo strategijoje numatytas įgyvendinti priemones (ar į naują kibernetinio saugumo strategiją, kuri bus parengta po galiojančios strategijos įgyvendinimo) įtraukti šias priemones:

2.1 suformuoti esmines kibernetinio saugumo problemas svarstančią ir siūlymus dėl jos teikiančią komisiją (darbo grupę), į kurios sudėtį, be strategijoje numatytas priemones vykdančių subjektų – viešojo sektoriaus institucijų atstovų, būtų įtraukti privataus sektoriaus atstovai, taip pat akademinės bendruomenės nariai. Nustatyti, kad komisija priima rekomendacinio pobūdžio sprendimus, posėdžiai organizuojami kas pusmetį ar pagal poreikį;

2.2 įdiegti platformą, kurioje asmenys galėtų anonimiškai pasikonsultuoti dėl patirtų kibernetinių incidentų ar veikų, galinčių būti kvalifikuotomis kaip elektroniniai nusikaltimai, gauti profesionalių patarimų. Į konsultacijų teikimo veiklą įtraukti gabius studentus (savanorystės ar praktikos atlikimo pagrindu);

3. Siūlytina plėsti ir konkretizuoti subjektų, teikiančių siūlymus dėl kibernetinio saugumo strategijos ir į jos įgyvendinimo priemonių planą įtrauktinų priemonių, grupę. Ypatingą dėmesį skirti akademinės bendruomenės siūlymams ir rekomendacijoms. Siekiant išvengti vien deklaratyvaus atsižvelgimo į gautus siūlymus, būtina numatyti jų nagrinėjimo ir sprendimo dėl (ne)atsižvelgimo į juos priėmimo mechanizmą.

4. Tobulinti ataskaitų už strategijoje numatytų priemonių įgyvendinimą teikimo ir vertinimo sistemą, Nacionaliniam kibernetinio saugumo centrui suteikiant ilgesnį terminą gautų ataskaitų vertinimui, taip pat numatant, kad visi ataskaitų vertinime dalyvaujantys subjektai (Nacionalinis kibernetinio saugumo centras, Krašto apsaugos ministerija, Vyriausybė) bet kada galėtų gauti trūkstamą informaciją tiesiogiai iš vykdytojų.

LITERATŪRA

Mokslo šaltiniai:

1. R. Baldoni. The future of Cybersecurity in Italy: Strategic focus areas. Laboratorio Nazionale di Cybersecurity, 2018.

2. W. Brenner S.W. Cybercrime: Criminal Threats from Cyberspace.// Library of Congress Cataloging, 2010.

3. E. F. Chamorro, J. R. C. Fernandez, R. M. Lopez, S. L. Fernandez „National Cyber Security, a commitment for everybody“, 2012.

4. Daniel R. Coats, „World wide threat assessment of the US intelligence community“, 2019.

5. J. Goodrich, “Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy,” in China and Cybersecurity: Political, Economic, and Strategic Dimensions, Report from workshops held at the University of California, San Diego (April 2012), 5-6. Prieiga internetu: http://igcc.ucsd.edu/assets/001/503568.pdf.

6. A. Graželis „Kovų arena – kibernetinė erdvė“. Kibernetinio saugumo apžvalga, 2016 m.

7. A. Komar „Tinklų ir informacinių sistemų saugumo direktyva – didžiulės ambicijos ir neapibrėžtos priemonės“. Kibernetinio saugumo apžvalga, 2016 m.

8. J. Kulys „Trumpa įžanga į kibernetinį saugumą“. Apžvalga, 2019-05-02. Prieiga internetu: http://apzvalga.eu/trumpa-izanga-i-kibernetini-sauguma.html.

9. G. Meškauskas „Nepatingėkite užduoti kontrolinio klausimo“. 2015 m. liepos 3 d. publikacija internete. Prieiga: https://www.bernardinai.lt/2015-07-03-g-meskauskas-nepatingekite-uzduoti-kontrolinio-klausimo/.

10. Joseph J. Panetta & R. Andrew Schroth. Cybersecurity Act of 2015 review. What it Means for Cybersecurity Governance and Enterprise Risk Management. Kogod School of Business, Washington, 2015.

11. A. Petrauskaitė, R. Markelienė, R. Gedminienė „Šalies saugumas ir gynyba“, Vilnius 2016.

12. S. Rothenpieler, International Relations Advisor, Federal Office for Information Security (BSI), National Cyber Security Strategy 2016. Prieiga internetu: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/april-2017/170426-bsi-enisa-nlo-presentation-v2.pdf.

13. P. Saudargas “Kibernetinių atakų Lietuvoje atvejai ir kaip į juos reaguojama“. Kibernetinio saugumo apžvalga, 2016.

14. Shoemaker, D. and Conklin, A. 2012. Cybersecurity: the Essential body of knowledge. Course technology.

15. S. Sloan, A Record Investment to Provide a More Secure Online World for All Australians, 2020. Prieiga internetu: https://blog.paloaltonetworks.com/2020/08/policy-australia-2020-cyber-security-strategy/.

16. Andrei Soldatov and Irina Borogan „Russia's approach to cyber: the best defence is a good offence". Hacks, leaks and disruptions Russian cyber strategies, Challot Papers, 2018.

17. D. Štitilis „Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos". Socialinės technologijos, 2013, 3(1).

18. D. Štitilis, P. Pakutinskas, M. Laurinaitis, I. Malinauskaitė–van de Castel. Lietuvos kibernetinio saugumo strategijos modelis. Mykolo Romerio universitetas, Vilnius, 2017.

19. D. Štitilis, P. Pakutinskas, M. Laurinaitis, I. Malinauskaitė–van de Castel. Rekomendacijos Lietuvos Respublikos kibernetinio saugumo įstatymui. Mykolo Romerio universitetas, Vilnius, 2017.

20. Warring State: Chinas Cybersecurity Strategy. Amy Chang, Center for a New American Security, 2014.

Teisės aktai:

21. Assessment of the EU 2013 Cybersecurity Strategy. European Commission, Brussels, 13.9.2017. Prieiga internetu: https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF.

22. Australia's Cyber Security Strategy, 2016. Prieiga internetu: https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf.

23. Australia's Cyber Security Strategy, 2020. Prieiga internetu: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

24. Cyber Security Strategy, Australia, 2009. Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AGCyberSecurityStrategyforwebsite.pdf.

25. Cyber Security Strategy for Germany, 2011. Prieiga internetu: https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1.

26. Cyber Security Strategy for Germany, 2016. Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Germany.

27. Convention on Cybercrime. Budapest, 23.XI.2001. Prieiga internetu: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

28. ENISA, National Cyber Security Strategies: *An Implementation Guide, 2012*. Prieiga: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.

29. ENISA, An evaluation framework for Cyber Security Strategies, 2014. Prieiga internetu: https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies.

30. ENISA, NCSS Good Practice Guide, 2016. Prieiga internetu: https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

31. EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace, BSA, 2015. Prieiga internetu: http://cybersecurity.bsa.org/index.html.

32. 2003 m. gruodžio 13 d. Europos saugumo strategija. Prieiga internetu: https://www.consilium.europa.eu/media/30821/qc7809568ltc.pdf.

33. 2013 m. vasario 7 d. svarstymui pateiktas direktyvos „Dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti“ projektas. Prieiga internetu: EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive | Shaping Europe’s digital future (europa.eu).

34. 2013 m. Europos Sąjungos kibernetinio saugumo strategija „Atvira, saugi ir patikima kibernetinė erdvė“. Prieiga: https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX:52013JC0001.

35. 2016 m. liepos 6 d. Europos Sąjungos direktyva 2016/1148 „Dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti“. Prieiga internetu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016L1148&from=LT.

36. Europos Sąjungos komisijos 2017 m. spalio 4 d. komunikatas „Racionaliausias tinklų ir informacijos saugumas. Kaip veiksmingai įgyvendinti Direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti”. Prieiga: https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52017DC0476&from=en.

37. 2020–2025 m. Europos Sąjungos kibernetinio saugumo strategija. Prieiga internetu: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

38. Europos Sąjungos Tarybos 2021 m. kovo 22 d. pranešimas spaudai „Kibernetinis saugumas: Taryba priėmė išvadas dėl Europos Sąjungos kibernetinio saugumo strategijos“. Prieiga internetu: https://www.consilium.europa.eu/lt/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/.

39. Finland Security Strategy for Society, 2010. Prieiga internetu: https://www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf.

40. Finland National Cyber Security Strategy, 2013. Prieiga internete: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Finland.

41. France National Cyber Security Strategy 2015. Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=France.

42. Information System Defense and Security – France Strategy 2011. Prieiga: https://www.enisa.europa.eu/media/news-ems/Information_system_security_France_strategy.pdf/view

43. Italian Cybersecurity Action Plan, 2017. Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Italy.

44. Japan Information Security Strategy for Protecting the Nation, 2010. Prieiga internetu: https://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf.

45. Lietuvos Respublikos kibernetinio saugumo įstatymas Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/15e540727ac211e89188e16a6495e98c.

46. Lietuvos Respublikos Vyriausybės 2001 m. gruodžio 22 d. nutarimas Nr. 1625 „Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.157225?jfwid=32wf55g0.

47. Lietuvos Respublikos Vyriausybės 2006 m. birželio 19 d. nutarimas Nr. 601 „Dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo. Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.278475?jfwid=fhhu5mn3t.

48. Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796 patvirtinta Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011 – 2019 metais programa. Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.403385.

49. Lietuvos Respublikos Vyriausybės 2012 m. balandžio 25 d. nutarimas Nr. 468 “Dėl Lietuvos Respublikos Vyriausybės 2006 m. gruodžio 13 d. nutarimo Nr. 1266 „Dėl elektroninės informacijos saugos koordinavimo komisijos sudarymo“ pakeitimo“. Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.423375?jfwid=g979e52t4.

50. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 patvirtinta Nacionalinė kibernetinio saugumo strategija. Prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595.

51. Lietuvos Respublikos Vyriausybės 2019 m. liepos 3 d. nutarimas Nr. 709 “Dėl Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano patvirtinimo“. Nutarimo prieiga internetu: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/faeb5eb4a6c811e9aab6d8dd69c6da66?jfwid=dg8d31595.

52. National Cyberspace Security Strategy, China 2016. Prieiga internetu: https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

53. National Cyber Security Strategy, Portugal, 2015. Prieiga: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Portuguese_National_Cyberspace_Security_Strategy_EN.pdf.

54. National Cyber Security Strategy of the United Kingdom, 2016. Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=United%20Kingdom.

55. National Cybersecurity Strategy, South Korea, 2019. Prieiga: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf.

56. National Cybersecurity Strategy USA, 2018. Prieiga internetu: https://trummpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

57. NCSS Good Practice Guide, 2016. Prieiga internetu: https://www.enisa.europa.eu/publications/ncss-good-practise-guide.

58. New Zeland‘s Cyber Security Strategy, 2015. Prieiga internetu: https://dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy-december-2015.pdf

59. Portuguese National Cyber Security Strategy, 2019. Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Portugal.

60. Spanish National Cyber Security Strategy, 2019. Prieiga internetu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Spain.

61. UK cybersecurity strategy. Protecting and promoting the UK in a digital world. Prieiga internetu: https://www.gov.uk/government/publications/cyber-security-strategy.

62. USA International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. White House, 2011. Prieiga internetu: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

63. USA Cybersecurity Information Sharing Act, 2015. Prieiga internetu: https://www.congress.gov/114/bills/s754/BILLS-114s754es.pdf.

64. USA National Strategy to Secure Cyberspace, 2003. Prieiga internetu: https://georgewbush-whitehouse.archives.gov/pcipb/cyberspace_strategy.pdf.

Kiti šaltiniai:

65. Chinese Hackers Blamed for Massive Microsoft Server Hack. The Diplomat, March 10, 2021. Šaltinis internetu: https://thediplomat.com/2021/03/chinese-hackers-blamed-for-massive-microsoft-server-hack/.

66. Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. OECD, 2012. Prieiga internetu: https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

67. Europos saugumo strategijos įgyvendinimo ataskaita „Saugumo užtikrinimas besikeičiančiame pasaulyje. Prieiga internetu: https://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/LT/reports/104645.pdf.

68. IBM X-Force Threat Intelligence Index 2018. Prieiga internetu: www.justincolman.com/wp-content/uploads/2019/03/Threat-Intelligence-2018-IBM-X-Force.pdf.

69. IT news, by Justin Hendry, ACSC countered 2266 cyber security incidents last year, September 4, 2020. Prieiga internetu: https://www.itnews.com.au/news/acsc-countered-2266-cyber-security-incidents-last-year-552858.

70. Jungtinių Tautų Tarptautinė telekomunikacijų sąjunga, Globalus kibernetinio saugumo indeksas, 2018. Prieiga internetu: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

71. Lithuania takes the 4th position in the Global Cybersecurity Index. LtLife.lt, 2019 m. balandžio 2 d. publikacija: https://ltlife.lt/lt-life-english/lithuania-takes-the-4th-position-in-the-global-cybersecurity-index/.

72. Social Media Statistics for Australia, updated March'21. Prieiga internetu: https://www.genroe.com/blog/social-media-statistics-australia/13492.

73. The cost of incidents affecting CIIs. ENISA, August 2016. Prieiga internetu: https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis.

74. Trend Micro 2008 Annual Threat Roundup and 2009 Forecast. Prieiga internetu: http://hoffmanmarcom.com/docs/Annual_Security_Threat_Report.pdf.

75. 2015 m. gruodžio 9 d. Valstybinio audito ataskaita Nr. VA-P-90-4-16 „Kibernetinio saugumo aplinka Lietuvoje".

76. U. S. National Cyber Strategy: What you need to know. Anastasios Arampatzis, 2018. Prieiga internetu: https://www.tripwire.com/state-of-security/government/us-cyber-strategy/.

SANTRAUKA

Kibernetinė erdvė ne tik suteikia naujų galimybių daugelyje gyvenimo sričių, bet ir sukelia pavojų, kurių pasekmės paliečia tiek atskirus individus, tiek valstybes. Kiekviena valstybė privalo prisiimti įsipareigojimus užkirsti kelią piktavališkiems veiksmams kibernetinėje erdvėje, todėl būtina sukurti nacionalinius kibernetinio saugumo pajėgumus (institucijas, įstatymus, procedūras) ir priimti būtiniausius įsipareigojimus, siekiant užtikrinti nacionalinės kibernetinės erdvės saugumą. Vienas iš pagrindinių dokumentų, kuriuo siekiama šio tikslo įgyvendinimo – valstybės kibernetinio saugumo strategija, nustatanti tiek esminius kibernetinio saugumo užtikrinimo principus, tikslus, prioritetus, tiek detalius kibernetinio saugumo priemonių įgyvendinimo planus.

Kibernetinėms grėsmėms vystantis ir sparčiai augant jų skaičiui, kibernetinio saugumo politika tampa nacionalinės politikos prioritetu. Kibernetinis saugumas priskiriamas prie kitų nacionalinių grėsmių, pvz., karo, todėl nacionalinių kibernetinio saugumo strategijų, numatančių efektyvių saugumo priemonių kūrimą ir diegimą, būtinas.

Pirmajame šio darbo skyriuje analizuojami nacionalinių kibernetinio saugumo strategijų poreikio kilimo istoriniai aspektai, pirmieji valstybių žingsniai kuriant ir diegiant savo nacionalines kibernetinio saugumo strategijas.

Antrasis skyrius skirtas pasirinktų valstybių (10) nacionalinių kibernetinio saugumo strategijų analizei, jų privalumų ir trūkumų įvertinimui, priemonių, gerosios patirties įgyvendinant atskiras strategijose numatytas priemones apžvalgai. Taip pat šiame skyriuje analizuojamas 2013 m. Europos Sąjungos kibernetinio saugumo strategijos turinys.

Trečiajame skyriuje analizuojama Lietuvos patirtis, kuriant ir diegiant kibernetinio saugumo strategijas, nagrinėjamas 2018 m. patvirtintos Nacionalinės kibernetinio saugumo strategijos turinys, joje numatytų priemonių įgyvendinimo perspektyvos.

Ketvirtajame skyriuje pateikiamas kibernetinio saugumo strategijos modelio pavyzdys, parengtas remiantis pasirinktų užsienio valstybių geroja praktika.

SUMMARY

Cyberspace not only offers new wide opportunities in many different life areas, but also poses dangers whose consequences affect both individuals and states. Each state must make a commitment to prevent malicious activity in cyberspace, and therefore is obligated to establish national cyber security capabilities (institutions, laws, procedures) and adopt commitments to ensure the security in cyberspace. One of the main documents whose aim is to achieve this goal is the State Cyber Security Strategy. The Strategy sets out both the essential principles, goals, priorities and detailed plans for the implementation of cybersecurity measures.

As cyber threats evolve and grow rapidly, cyber security policy has become a nationals policy priority. Cyber security is one of the other national threats, such as war, therefore national cyber security strategies, that provide the development and implementation of effective security measures, are essential.

The first chapter of this wok analyses the historical aspects of the rise in the need for national cyber security strategies, first steps, which governments take in order to develop and implement their national cyber security strategies.

The second chapter is dedicated to the analysis of the selected countries (10) national cyber security strategies, the assessment of their strengths and weaknesses, and the review of measures and good practices in the implementation of individual measures provided in the strategies. The content of the 2013 European Union cyber security strategy is also discussed.

The third chapter analyses Lithuania's experience in developing and implementing cyber security strategies, also the content of the National Cyber Security Strategy, implemented during 2018–2023 period, perspectives for the implementation of the measures provided in this document.

The fourth chapter presents an example of a cyber security strategy model based on the best practices of selected foreign countries.

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2021-05-03

Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas), Viešojo valdymo ir verslo fakulteto kibernetinio saugumo valdymo programos studentė Giedrė Ūdraitė, patvirtinu, kad šis magistro baigiamasis darbas „Kibernetinio saugumo nacionalinių strategijų kūrimo ir diegimo ypatumai: pasaulio šalių analizė“:

1. Yra atliktas savarankiškai ir sąžiningai;

2. Nebuvo pristatytas ir gintas kitoje mokslo įstaigoje Lietuvoje ar užsienyje;

3. Yra parašytas remiantis akademinio rašymo principais ir susipažinus su rašto darbų metodiniais nurodymais.

Man žinoma, kad už sąžiningos konkurencijos principo pažeidimą – plagijavimą studentas gali būti šalinamas iš Universiteto kaip už akademinės etikos pažeidimą.

_____ Giedrė Ūdraitė