MYKOLO ROMERIO UNIVERSITETAS

VERSLO IR MEDIJŲ MOKYKLA

(BUSINESS AND MEDIA SCHOOL (BMS))

GODA UŽKURAITYTĖ

Kibernetinio saugumo valdymas

KIBERNETINIO SAUGUMO VALDYMO UŽTIKRINIMAS: PASAULINĖ PATIRTIS IR LIETUVOS PERSPEKTYVA

Magistro baigiamasis darbas

Darbo vadovas –

Doc. Dr. Tadas Limba

Vilnius, 2015

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

ĮVADAS

Temos aktualumas ir naujumas. Informacinių technologijų ir komunikacijų plėtra daro didžiulę įtaką visuomenei pastaraisiais dešimtmečiais. Lemiamos reikšmės tai turi tiek žmogui, kaip atskiram individui, tiek ir visai visuomenei bei verslui. Internetas svarbus ir organizaciniu lygiu, nes vis daugiau operacijų yra atliekama interneto pagalba. Sparti informacinių technologijų plėtra lėmė tai, kad internetas tapo pagalbine ir neatsiejama priemone. Informacinės sistemos tapo neatsiejama gyvenimo ir verslo dalimi. Vis daugiau ir daugiau kasdienės veiklos, paslaugų yra perkeliama į virtualią erdvę, tokiu būdu siekiant palengvinti verslo procesus, o taip pat padidina galimybes greitai ir kokybiškai dalintis informaciniais ištekliais. Įmonės stengiasi integruoti savo veikloje informacines technologijas siekdamos tapti konkurencingomis bei didinti savo veiklos efektyvumą. Interneto dėka, laikas ir atstumas neteko prasmės - elektroninė erdvė yra globali.

Deja, internetas atnešė ne tik milžinišką naudą. Būtent elektroninės erdvės globalumas suteikė sąlygas vykdyti nusikaltimus iš bet kurios pasaulio vietos ir bet kuriuo paros laiku. Elektroniniai nusikaltimai tapo įprasto nusikalstamumo dalimi. Jie teikia tokias pat neigiamas pasekmės kaip ir tie nusikaltimai, kurie yra atliekami fizinėje erdvėje. „Visuotinis informacinių technologijų naudojimasis paskatino ir didėjantį kibernetinių atakų skaičių. 2013 metais daugiau nei 40 mln. žmonių Jungtinėse Amerikos Valstijose, 54 mln. Turkijoje, 20 mln. Korėjoje, 16 mln. Vokietijoje ir daugiau nei 20 mln. žmonių Kinijoje patyrė kibernetinius išpuolius.“ (Center for Strategic and International Studies & McAfee, 2014).

Kibernetiniai išpuoliai privertė šalis imtis prevencinių priemonių norint nuo jų apsisaugoti. Kibernetinio saugumo klausimas tapo aktualus siekiant apsaugoti nacionalinę šalių kibernetinę erdvę. Tam tikslui yra kuriamos kibernetinio saugumo strategijos ir programos. Oksfordo žodynas apibrėžia strategiją kaip veiksmų planą, kuris yra sukurtas norint pasiekti ilgalaikio arba bendro tikslo (Oxford English Dictionary, 2012). Pagrindinis kibernetinio saugumo strategijų tikslas yra apsauga nuo netinkamo tinklų infrastruktūros naudojimo: atsparumo didinimas, informacijos ir komunikacijos technologijų apsauga, kritinių infrastruktūrų saugumo užtikrinimas. „Elektroninės erdvės globalumas sukūrė beprecedentes sąlygas daryti nusikaltimus iš bet kurio pasaulio taško, kuriame yra internetas. Todėl labai svarbu apsisaugoti nuo elektroninių nusikaltimų, vykdomų pasitelkiant internetą. Kibernetinis saugumas tampa vienu iš pagrindinių tikslų, turint omenyje, kad grėsmės elektroninėje erdvėje kyla ne tik atskiriems vartotojams, bet net valstybėms“(Štitilis, 2013).

Kompiuteriniai tinklai bei sistemos, kuriais naudojamės ir kuriais yra perduodama svarbi bei slapta informacija privalo nuolatos būti saugomi. Kibernetinis saugumas privalo būti užtikrintas tiek viešajame, tiek ir privačiajame sektoriuje. „Kiekvienais metais pasaulio valstybės išleidžia milijardus eurų ir dolerių kovai su kibernetinėmis atakomis ir jų padariniams likviduoti.

Valdiškuose kompiuteriuose tyliai guli terabaitai informacijos, kurią praradus gresia katastrofiški padariniai. Nuo karinių paslapčių iki piliečių socialinio draudimo kortelių numerių, nuo slaptas misijas atliekančių pareigūnų pavardžių iki įvaikintų vaikų sąrašų“ (Daugelio kibernetinių grėsmių sukėlėjai – patys valdininkai, 2014).

Pasak Lietuvos Respublikos Nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio (CERT-LT) duomenimis, per metus Lietuvoje įvyksta virš 25 tūkst. incidentų, susijusių su kibernetiniu saugumu, didžioji dalis jų kyla dėl nusikalstamos veiklos iš užsienio. Taigi, tarpusavio bendradarbiavimas ir dalijimasis gerąja praktika yra vienas iš svarbiausių aspektų norint užtikrinti atvirą, saugią ir patikimą kibernetinę erdvę.

Tyrimo objektas. Kibernetinio saugumo valdymo užtikrinimas.

Mokslinė problema. Mokslo šaltiniuose nepakankamai išanalizuoti kibernetinio saugumo užtikrinimo metodai ir tiksliai neapibrėžtas teisinis reguliavimas gali lemti kibernetinio saugumo stoką Lietuvoje.

Tyrimo tikslas. Išanalizuoti esamą situaciją ir priemones tarptautiniu mastu, t. y. išanalizuoti pasirinktų šalių kibernetinio saugumo strategijas pagrindinius principus ir priemones bei pritaikyti juos formuojant saugią Lietuvoje kibernetinio saugumo politiką.

Pagrindiniai uždaviniai:

1. Išanalizuoti kibernetinio saugumo valdymo teorinius aspektus;
2. Išnagrinėti kibernetinio saugumo valdymo pasaulinę patirtį;
3. Išsiaiškinti kibernetinio saugumo valdymo situaciją Lietuvoje;
4. Atlikti kibernetinio saugumo užtikrinimo Lietuvoje tyrimą.

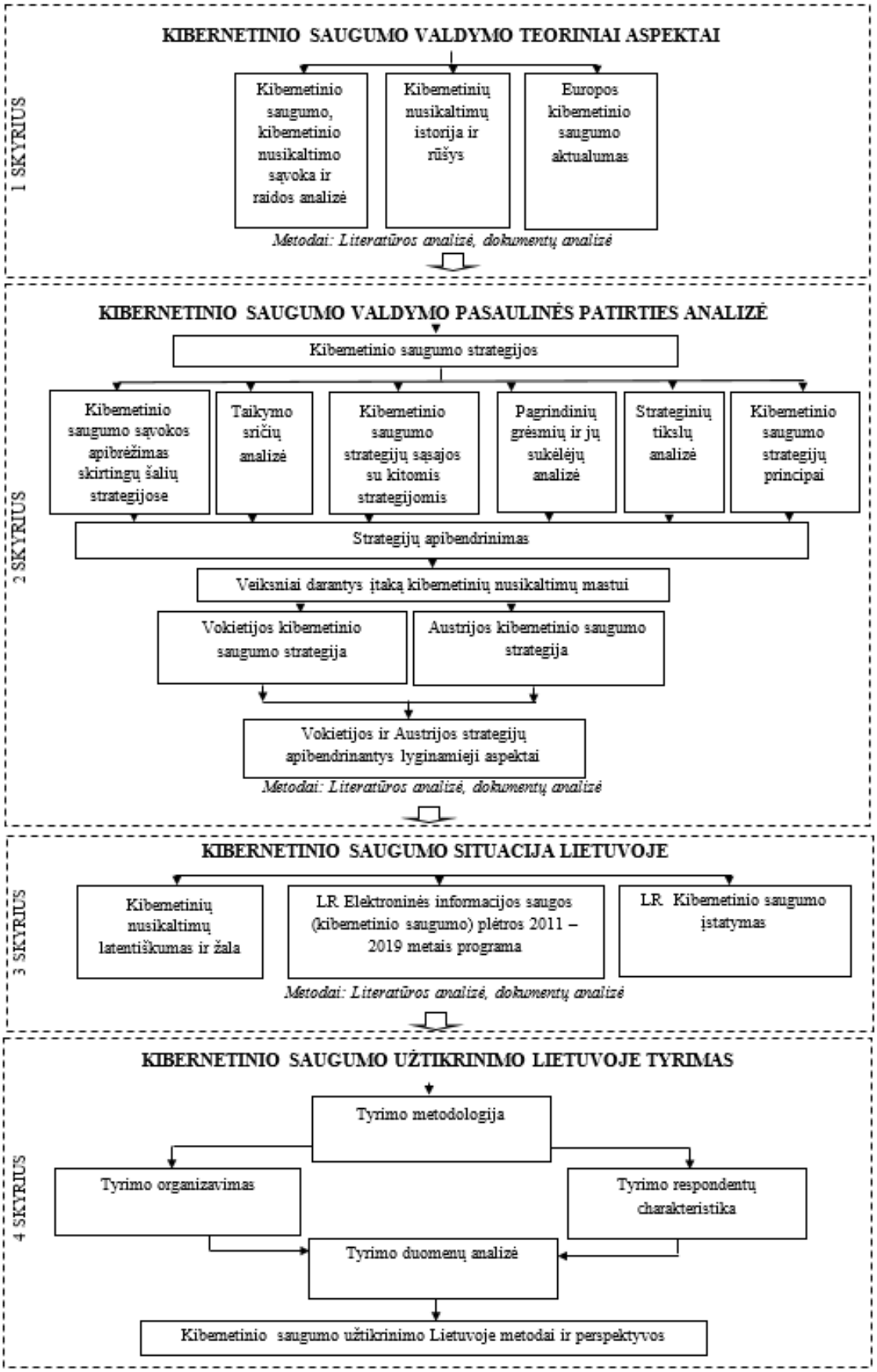
Ginamieji teiginiai:

1. Kibernetinio saugumo teisinio reguliavimo trūkumas lemia kibernetinio saugumo problemą Lietuvoje.
2. Kibernetinio saugumo valdymo metodų trūkumas lemia neefektyvų incidentų valdymą.

Darbos šaltiniai ir metodai. Darbe buvo atlikta išsami mokslinės literatūros bei dokumentų turinio analizė kibernetinio saugumo srityje. Remiantis užsienio šalių strateginiais dokumentais (Kanados, Jungtinių Amerikos Valstijų, Prancūzijos, Čekijos, Naujosios Zelandijos, Austrijos ir Vokietijos kibernetinio saugumo strategijomis buvo atlikta lyginamoji analizė. Tiriant Lietuvos situaciją kibernetinio saugumo srityje buvo analizuojami Lietuvos Respublikos teisės aktai, reglamentuojantys kibernetinį saugumą (Lietuvos Respublikos kibernetinio saugumo plėtros 2011 – 2019 metais programa, Lietuvos Respublikos kibernetinio saugumo įstatymas)**,** naudoti kokybinių ir kiekybinių duomenų rinkimo metodai analizuojant Lietuvos statistinius duomenis, o taip pat buvo atliktas kokybinis ekspertų interviu.

Darbo struktūra. Magistro baigiamąjį darbą sudaro keturi pagrindiniai skyriai (žr. Pav. 1). Pirmame skyriuje yra analizuojami kibernetinio saugumo teoriniai aspektai, analizei naudojamos mokslinės knygos ir moksliniai žurnalai, interneto medžiaga. Antrame skyriuje yra analizuojama pasaulinė patirtis kibernetinio saugumo srityje, atlikta pasirinktų valstybių kibernetinio saugumo strategijų analizė, pateiktos išvados. Trečiame skyriuje analizuota kibernetinio saugumo situacija Lietuvoje, atskleistos problemos. Trečiame skyriuje išanalizuotos pagrindinės problemos, kurios ketvirtame etape pristatytos ekspertams - atliktas kokybinis tyrimas, naudotas ekspertų interviu metodas. Ekspertų interviu metodu siekta išanalizuoti ir įvertinti kibernetinio saugumo situaciją ir perspektyvas Lietuvoje.

Tyrimo praktinis reikšmingumas. Tyrimo rezultatai gali būti pritaikyti siekiant tobulinti Lietuvos kibernetinio saugumo užtikrinimą, ypač pabrėžiant empirinius tyrimo rezultatus.



Pav. 1 **Magistro baigiamojo darbo struktūros loginė schema**

KIBERNETINIO SAUGUMO VALDYMO TEORINIAI ASPEKTAI

1.1 Kibernetinio saugumo, kibernetinio nusikaltimo sąvoka ir raidos analizė

Kibernetinis (elektroninio) saugumo užtikrinimas tampa vis aktualesnė šių dienų problema. Niekas nenori, kad jiems svarbi ar konfidenciali informacija taptų viešai prieinama, ar būtų naudojama piktaviliškai. Be abejo, vartotojams yra svarbi informacija kurią jie naudoja. Tačiau interneto erdvėje kaip ir realiame gyvenime - interneto naudotojai bendrauja, dirba, perka ir vykdo kitus elektroninius procesus taigi visi šie procesai privalo būti apsaugoti.

Kibernetiniai ginklai (atakos, incidentai elektroninėje erdvėje), nors iš pirmo žvilgsnio taip ir neatrodo, yra tokie pat pavojingi kaip ir fiziniai ginklai, pavyzdžiui, kariniai lėktuvai ar naujo tipo amunicija, kuri skrieja toliau, greičiau, taikliau arba smarkiau sužaloja priešininką. Norint turėti karinį pranašumą prieš priešininkus, būtina išmanyti apie visas priemones – net ir tas, kurios neatrodo tokios pavojingos. Tos priemonės, kurios dažniausiai yra nematomas (todėl, galbūt ir neatrodo tokios pavojingos), gali būti panaudotos taip sėkmingai, kaip negalėtų būti panaudota net didžiulė karių grupuotė. Lietuvos Respublikos kibernetinio saugumo įstatyme kibernetinis incidentas apibrėžtas kaip „įvykis ar veika, kuri sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos, sutrikdyti ar pakeisti, įskaitant valdymo perėmimą, informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims“ (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014). 17 metų Užsienio reikalų ministerijos (URM) sistemoje dirbęs S. Japertas siūlo remtis NATO arba JAV apibrėžimais. „Kibernetinę ataką galima suprasti kaip kibernetinę karo formą, naudojamą su fizine ataka arba be jos. Jos tikslas yra suardyti priešininkui priklausančias informacines sistemas“ (Japertas, 2010).

2010 m. sausį įvyko sukrečiantis įvykis įėjęs į elektroninių nusikaltimų istoriją, kuomet teko pripažinti, kad kibernetinės atakos yra be galo pavojingos ir gali padaryti tokią pat žalą kaip ir fizinės išpuoliai. Kibernetinis išpuolis Natanze, Irane - tai vienas iš tokių atvejų, kai beliko tik stebėti kas vyksta ir bandyti pasisemti išminties bei išradingumo – sudėtinga kibernetinė ataka buvo įvykdyta urano sodrinimo bazėje. „Ši bazė nuo išorinių kibernetinių išpuolių buvo apsaugota, atrodytų, neįveikiamai – visi jos viduje esantys kompiuteriai buvo apsaugoti vadinamuoju „oro tarpu“. Kitaip tariant, nė vienas iš jų nebuvo kokiais nors tinklais sujungtas su išoriniu pasauliu. Bet pasitelkus

išradingumą kompiuterinis virusas „Stuxnet“ sugebėjo patekti į bazę, o tada, automatiškai nusitaikęs į „Siemens“ aparatūros valdymo sistemas, pradėjo chaotiškai kaitalioti urano sodrinimo centrifugų sukimosi greitį ir tokiu būdu apie 1000 jų sugadino“ (Zetter, 2014). Kibernetinės atakos gali būti pražūtingos, todėl yra būtina turėti gynybos planą, kuris užtikrintų kibernetinį saugumą ir neleistų „Stuxnet“ istorijai kartotis. „Saugumo ekspertai sako, kad šis kompiuterinis virusas galėjo būti valstybės finansuotas išpuolis prieš Irano branduolinę programą ir galėjo kilti Jungtinėse Amerikos Valstijose ar Izraelyje“ (Kelley, 2013).

Lietuvos Respublikos kibernetinio saugumo įstatyme kibernetinis saugumas apibrėžtas kaip visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti“ (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

Pasak Lietuvos Respublikos ryšių reguliavimo tarnybos, „kibernetinis saugumas paprastai suprantamas kaip apsauga nuo neteisėtos prieigos prie informacijos, jos panaudojimo, keitimo, manipuliavimo, praradimo. Bendrąja prasme saugumas - tai būsena, kai negresia joks pavojus. Tačiau absoliutaus saugumo pasiekti neįmanoma, bet tinkamai parinktos ir taikomos saugumo priemonės gali sumažinti rizikos laipsnį ir praradimų mastus“.

1.2 Elektroninių nusikaltimų istorija ir rūšys

Kartu su kompiuterinių technologijų karta 20 amžiuje prasidėjo ir kibernetinių (elektroninių) nusikaltimų istorija. Augančioje kompiuterinėje visuomenėje atsirado žmonių, kurie siekdami naudos sau, pradėjo kenkti visuomenei pasitelkdami kompiuterines technologijas. Neilgai trukus piktnaudžiavimas elektroninėje erdvėje išplito į verslo ir privatųjį sektorių. Problema tapo išties jautri kai piktavaliai pradėjo kenkti ypatingos svarbos informacinėms infrastruktūroms[1].

Vienas iš pirmųjų, kuris susidomėjo elektroninių nusikaltimų problema buvo Donas Parkeris – informacijos saugumo konsultantas iš JAV. D. Parkeris turi daugiau nei 50 m. siekiančią patirtį kompiuterių programavimo, kompiuterinių sistemų valdymo, konsultavimo, mokslinių tyrimų srityje. Jis kompiuterinį nusikaltimą apibrėžė kaip tyčinę veiką, kuri vienaip ar kitaip yra susijusi su kompiuteriu ir dėl kurios auka patyrė ar galėjo patirti žalos, o nusikaltėlis gavo, arba galėjo gauti naudos.

[1] *Ypatingos svarbos informacinė infrastruktūra (kritinė infrastruktūra) – elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, nepaisant to, ar jos valdytojas yra privatus ar viešojo administravimo subjektas, kuriuose įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams* (LR kibernetinio saugumo įstatymas, 2014).

Pirmasis kibernetinis incidentas buvo užfiksuotas 1958 m. Po šio incidento sekė daugybė kitų incidentų kibernetinėje erdvėje, tokių kaip vagystės, apgaulės, sukčiavimai, neteisėti duomenų pasisavinimai, turto prievartavimai, sabotažai, šnipinėjimai, pagrobimai, žmogžudystės ir daugybė kitų. „Pirmasis kibernetinis nusikaltimas JAV (buvo atliktas neteisėtas banko įrašų keitimas Mineapolyje, Minesotos valstijoje), kurio organizatorius buvo persekiojamas federaliniu mastu, buvo įvykdytas 1966 m.“ (Parker, 1989). „Pirmoji internetinė žmogžudystė (žmogžudystė, kuomet buvo pasinaudota internetine erdve kurioje auka ir nusikaltėlis užmezgė kontaktą) buvo įvykdyta 1996 m.“ (Singh, 2008).

„Elektroninius nusikaltimus galima apibrėžti kaip nusikaltimus, kurių metu yra naudojamas kompiuteris ir internetas“ (Moore, 2005). Dr. D. Halder ir K. Jaishankar elektroninius nusikaltimus sąvoką apibrėžė kaip „veiką, kuri yra atliekama pavienių asmenų ar asmenų grupių, turint nusikalstamą motyvą, siekiant aukai padaryti fizinę ar moralinę žalą (pvz.: sugadinti reputaciją) naudojantis telekomunikacijų tinklais, tokiais kaip internetas (pvz.: pažinčių svetainės (angl. *chat rooms*), elektroninis paštas, pokalbių forumai grupės (angl. *notice boards and groups*), o taip pat ir mobiliaisiais telefonais (SMS/MMS)) “. Kompiuteris gali būti naudojamas kaip nusikaltimo įrankis, arba nusikaltimo objektas.

Griežtai apibrėžtos ir vienareikšmiškos sąvokos autoriai nepateikia. Literatūroje taip pat naudojami skirtingi terminai apibrėžiantys kibernetinius incidentus: “kibernetinis nusikaltimas”, “kompiuterinis nusikaltimas”, “aukštų technologijų nusikaltimas” ir t.t. Budapešto Konvencijoje dėl elektroninių nusikaltimų, dažniausiai naudojama „elektroninio nusikaltimo“ sąvoka. Konvencijoje dėl elektroninių nusikaltimų yra išskiriamos keturios pagrindinės elektroninių nusikaltimų rūšis:

1. **Nusikaltimai kurie pažeidžia kompiuterinių duomenų ir kompiuterinių sistemų konfidencialumą, vientisumą ir prieinamumą:**

- Neteisėta prieiga prie kompiuterinės sistemos ar jos dalies (pavyzdžiui: šnipinėjimas, neteisėtas duomenų kopijavimas, sukčiavimas ir t.t.). „Neteisėta prieiga prie kompiuterių programų arba duomenų elektronine forma laikytina tokia veikla, kuri pažeidžia laikomos informacijos slaptumą (t. y. kyla realios žalos grėsmė), o dėl neteisėtos prieigos vykdomas šnipinėjimas, neteisėtai kopijuojami autorių teisėmis apsaugoti kūriniai, sabotažas, sukčiavimas, naudojantis kompiuteriais ir pan. laikytini savanoriškomis pavojingomis veikomis“ (Štitilis, 2011).

  Įdomu tai, kad jau 1985 m. Austrijoje, Vienoje studentas įsilaužė į kelias finansines įstaigas. Jokios žalos jis nepadarė, tačiau apie šį incidentą buvo pranešta atitinkamoms institucijoms. Tyrimas vėliau buvo nutrauktas, kadangi žala nebuvo padaryta. Šis studento „žygdarbis“ buvo prilygintas „intelektiniam iššūkiui“. Būtent dėl šios priežasties

didžiosios informacinių technologijų kompanijos (pvz.: Google) stengiasi pasamdyti programišius, kurie yra „nulaužę“ kompanijos sistemas. Kompanija „Google“ pranešė, kad pasamdė programišių George'ą Hotzą, kuris 2007 m. nulaužė „iPhone“ operacinę sistemą. George‘as Hotzas tapo kompanijos saugumo ekspertų komandos „Project Zero“ nariu.

- Sąmoningas neteisėtas neviešų kompiuterinių duomenų perdavimas techninėmis priemonėmis į kompiuterinę sistemą, taip pat elektromagnetinės emisijos iš kompiuterinės sistemos, kuri perduoda kompiuterinius duomenis perimtis.
- Sąmoningas neteisėtas kompiuterinių duomenų sugadinimas, sunaikinimas, apgadinimas, pakeitimas arba galimybės naudotis duomenimis panaikinimas.
- Netinkamas įtaisų naudojimas (įskaitant ir kompiuterinę programą), siekiant įvykdyti aukščiau nurodytus nusikaltimus. Netinkami įtaisus yra draudžiama gaminti, parduoti, įsigyti turint tinklą panaudoti, įvežti, platinti arba kitokiomis galimybėmis naudoti.

Elektroninėje erdvėje labiausiai paplitę metodai, darantys žalą, yra kenksmingų programų, kurios kopijuoja, ištrina, ar kitaip sugadina duomenis panaudojimai vartotojų kompiuterinėse sistemose. Tai gali būti kompiuterinis „virusas“, „kirminas“ (angl. *computer worm),* „Trojanas“ (dar kitaip vadinamas „Trojos arkliu“; angl. *Trojan Horse*), „loginė bomba“, ir kt. Kompiuterinis virusas tai kenksminga nedidelės apimties programa, kuri turi automatinį dauginimosi mechanizmą ir atliekanti vartotojo kompiuteryje nepageidaujamus veiksmus. Dažniausiai virusais užsikrečiama kai iš interneto parsisiunčiama nepatikimus (infekuotus) duomenis, taip pat dažnai užsikrečiama elektroniniu paštu plintant virusui, kuris dažnai būna „prisegtas“ prie siunčiamos nuotraukos, ar nuorodos. Kirminas yra panaši į virusą programa, kuri pati sugeba daugintis. Didžiausias jų keliamas pavojus yra jų sugebėjimas daugintis dideliais kiekiais. Įprastam virusui reikalingas įsiskverbimas į kitus failus, na, o kirminas gali daugintis nesustodamas tol, kol išnaudos kompiuterio duomenų talpą arba išplis po visą tinklą ir sutrikdys jo darbą. Daugiausia kirminai kaip ir virusai plinta elektroniniu paštu ir aktyvuojasi atidarius failą (dokumentas ar nuotrauka), kuris yra pridėtas prie laiško. Trojanai (dar kitaip vadinami Trojos arkliais) - tai kompiuterinės programos, besislepiančios kitose programose ir išoriškai atrodo kaip naudingos, tačiau realiai sukelia kenksmingus padarinius. Skirtingai nuo kirminų, Trojanai negamina savo kopijų, bet aktyvavus programą, po kuria jie slepiasi, kartu aktyvuojamas ir virusas. Veikiantis Trojanas ypatingai pavojingas, nes sudaro virtualų koridorių, per kurį užkrėstasis kompiuteris ir jo resursai tampa prieinami iš išorės. Užpuolę sistemą jie turi galimybę ištrinti bylas, sunaikinti kitą kietojo disko informaciją bei atidaryti prieigą pašaliniams vartotojams, pasiekti ir vogti informaciją iš užkrėsto kompiuterio. Pastaroji virusų galimybė ypač pavojinga, kadangi įmanoma, jog svarbi informacija

pateks į svetimas rankas, kompiuteris nebus kontroliuojamas jo šeimininko. Pasaulyje suskaičiuojama iki 10000 skirtingų virusų.

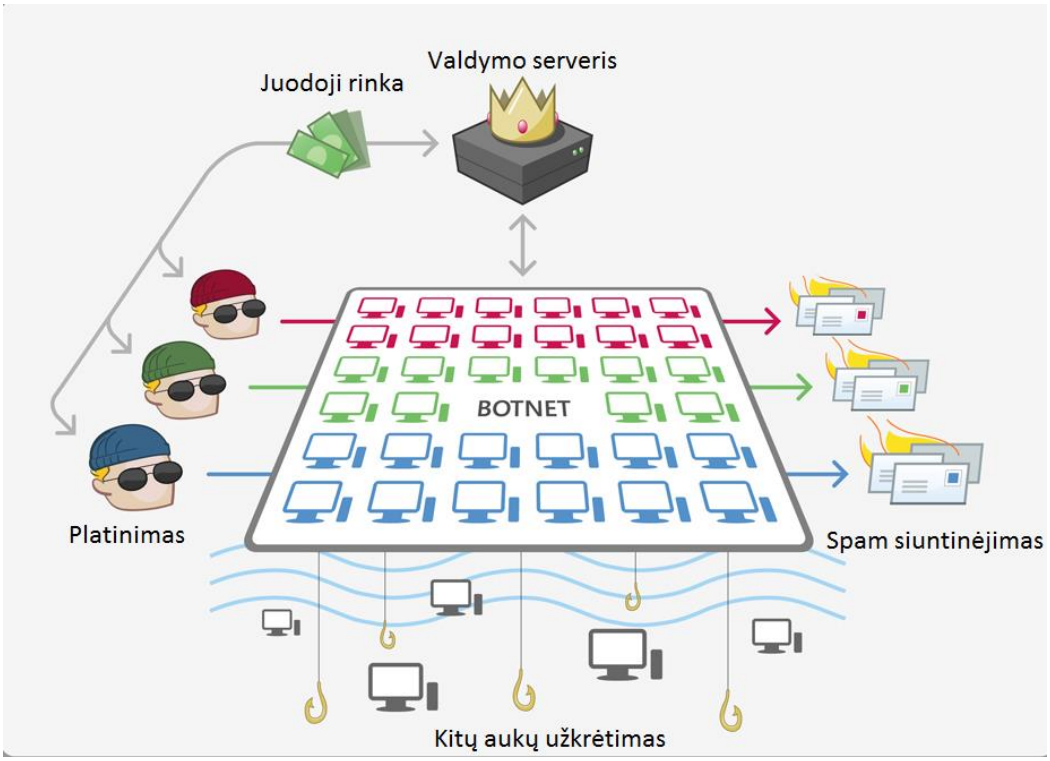
2. **Kompiuteriniai nusikaltimai.**

Kompiuterinis sukčiavimas apibrėžiamas kaip „pinigų arba kito turto grobimas naudojant kompiuterį“ (Štitilis, 2011). Sukčiavimus atliekant kompiuteriu galima būtų galima suskirstyti į dvi grupes:

- Sukčiavimas susijęs su duomenimis;
- Sukčiavimas susijęs su programomis.

Sukčiavimus atliekant kompiuteriu pasireiškia turto arba paslaugos gavimas apgaulės būdu (pavyzdžiui: nusikaltėlių nurodymai kompiuteriams pervesti aukos pinigus į tam tikras banko sąskaitas, neteisėti duomenų parsisiuntimai, duomenų klastojimai).

Tokių nusikaltimų pavydžiai galėtų būti kenkėjiškos programinės įrangos, sudaryti botnet tinklai. Tai tokie tinklai, kurie sudaromi užkrėtus daug kompiuterių ir vėliau juos panaudojant įvairioms, dažniausiai paskirstyto atsisakymo aptarnauti (*DDoS*), atakoms vykdyti. Auka ilgą laiką net nežino, kad jos kompiuteris yra įtrauktas į botnet tinklą, nes kompiuteris veikia normaliai, tiesiog retkarčiais gali sulėtėti interneto ryšys. Tiksliai nežinoma, kiek ir kokio dydžio „botnet“ tinklų šiuo metu egzistuoja internete. Botnet tinklas gali būti sudarytas iš kelių tūkstančių arba iš kelių milijonų užkrėstų kompiuterių. Spėjama, kad vienas iš 600 prie interneto prisijungusių kompiuterių pasaulyje priklauso kuriam nors botnet tinklui. Botnet tinklams sudaryti nusikaltėliai naudoja kenksmingą programinę įrangą, kompiuterius užkrečia per elektroninius laiškus, nuorodas internete. Aukai atidarius nuotrauką arba paspaudus ant nuorodos kompiuteris apkrečiamas. Užkrėsta sistema susisiekia su valdymo serveriu ir gauna komandų sąrašą. Vėliau užkrėsti kompiuteriai prisijungdami prie valdymo serverio pasitikrina ar nėra naujų užduočių. Botnet dažniausiai naudojami banko prisijungimo duomenų perėmimui, brukalų (angl. *spam*) siuntinėjimui (tai šiukšlės gaunamos elektroniniu paštu), sisteminių komandų vykdymui (norint atlikti DDos atakas (angl. *Distributed Denial of Service*), ir t.t. Botnet tinklo schema pateikta Pav. 6.



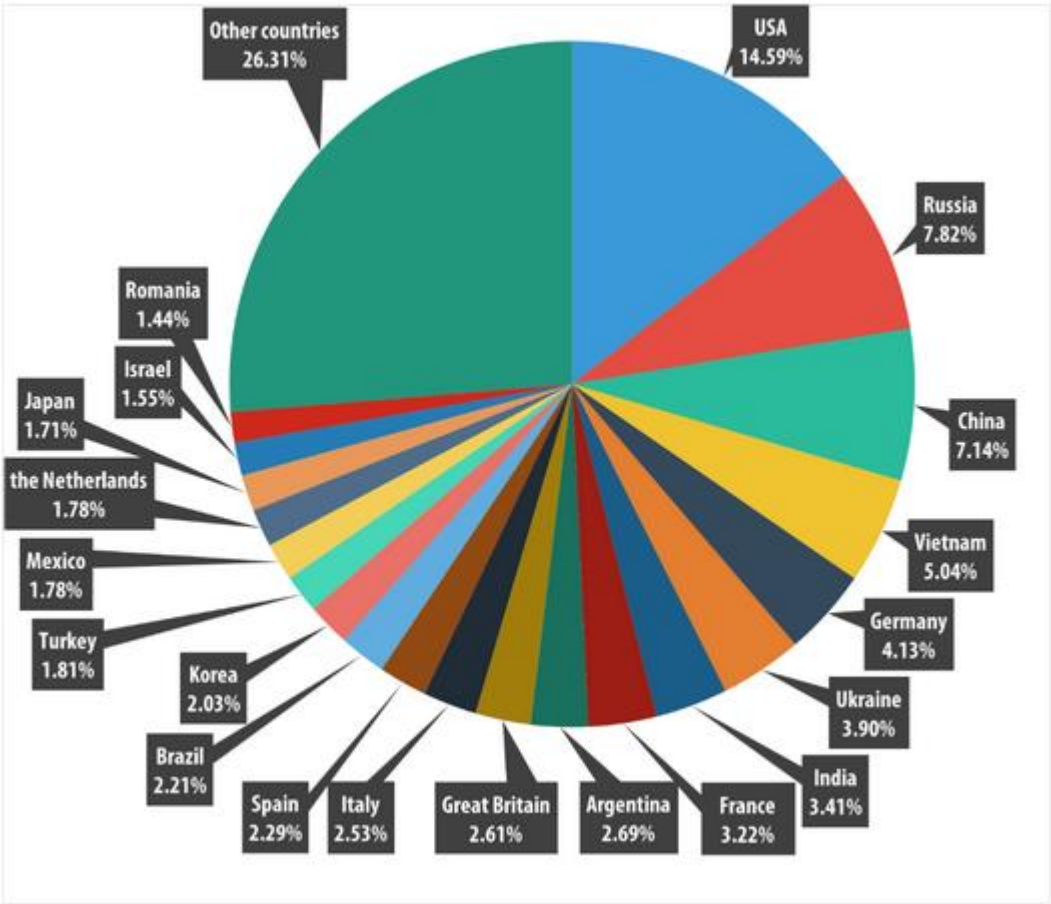
Šaltinis: http://www.esaugumas.lt/lt/botnetai.html

Pav. 2 **Botnet tinklo schema**

Kibernetiniai nusikaltėliai botnet tinklus naudoja norėdami patenkinti savo nelegalius tikslus. Pagrindinės botnet tinklų panaudojimo sritys yra šios:

- **Spam'ų siuntinėjimas** (liet. *nepageidaujami laiškai, brukalai*). Spam'ų siuntinėjimas yra viena populiariausių botnet tinklų panaudojimo funkcijų. Daugiau nei 80 proc. brukalų yra išsiunčiama pasinaudojus botnet tinklu.

„Karspersky lab" duomenimis, 2015 m. antrąjį ketvirtį, daugiausia nepageidaujamų laiškų buvo išsiųsta iš Jungtinių Amerikos Valstijų (14,59 proc.) ir Rusijos (7,82 proc.). Iš Kinijos buvo išsiųsta 7,14 proc. viso pasaulio nepageidaujamų laiškų (lyginant su pirmuoju 2015 m. ketvirčiu, iš Kinijos siunčiamo *spam'o* srautas sumažėjo 3,23 proc.).



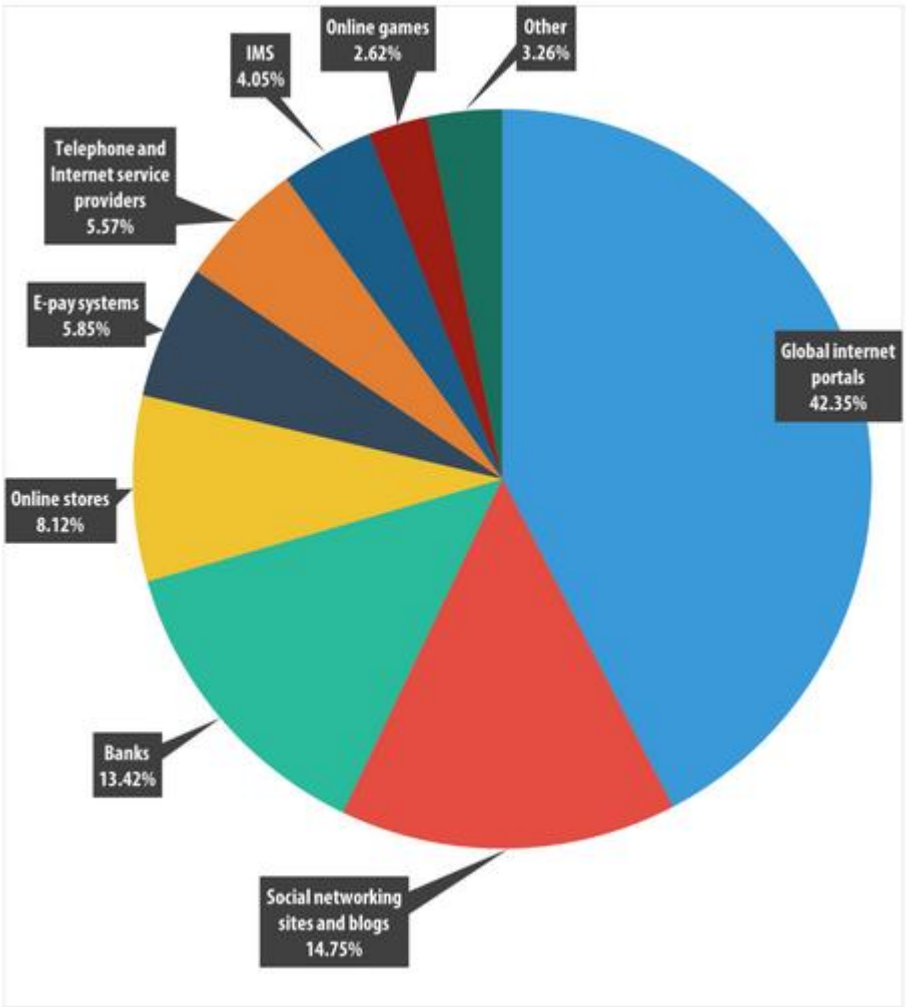
Šaltinis: Karspersky Lab report, „Spam & Phishing in Q2 2015“.
https://securelist.com/files/2015/08/KL_Q2_2015_SPAM_REPORT_ENG.pdf

Pav. 3 **Šalys, esančios nepageidaujamų laiškų šaltiniai, 2015 m. antrasis ketvirtis**

- **Šantažas kibernetinėje erdvėje**. Botnet tinklai dažnai yra naudojami vykdant DDos atakas (angl. *Distributed Denial of Service*) atakas. DDoS - paskirstyto atsisakymo aptarnauti atakos. DDos atakos metu botnet tinklo kompiuteriai siunčia didelį srautą „netikrų“ užklausų į nusikaltėlių atakuojamus internetinius serverius. Dėl per didelės apkrovos atakuojama paslauga tampa neprieinama vartotojams (pavyzdžiui: 2010 metais piktavaliai atakavo vienos Lietuvos kelionių agentūros tinklapį. Programišiai reikalavo išpirkos, kuri siekė 3 tūkst. eurų, tam, kad ataka būtų sustabdyta).
- Egzistuoja net gi **botnet tinklų prekyba arba nuoma** – programišiai pardavinėja arba nuomoja botnet tinklus kitiems nusikaltėliams atakoms vykdyti.
- **Phishing‘as** (angl. *phishing*). Phishing’u yra vadinamas internetinių svetainių klastojimas, siekiant gauti internetinių paskyrų duomenis ir iš to gauti finansinės naudos. Suklastotų interneto tinklapių talpinimas per botnet tinkluose esančius

kompiuterius sudaro galimybes kibernetiniams nusikaltėliams keisti tinklapių lokacijos vietas, tokiu būdu juos išlaikyti kuo ilgiau veikiančius (išvengiama blokavimo situacijos).

„Karspersky lab“ duomenimis, 2015 m. antrąjį ketvirtį daugiausia phishing‘o atakų sulaukė pasauliniai interneto portalai ir socialiniai tinklai: *Facebook* (10,44 proc.), *Google* (5,67 proc.), *Yahoo* (29,03 proc.). Suklastotos globalių pasaulio portalų versijos sudaro net 42,35 proc., na o socialiniai tinklai ir blogai sudaro 14,75 proc. visų phishing‘o paveiktų tinklapių.



Šaltinis: Karspersky Lab report, „Spam & Phishing in Q2 2015“.
https://securelist.com/files/2015/08/KL_Q2_2015_SPAM_REPORT_ENG.pdf

Pav. 4 **Phishing atakos organizacijose pagal kategorijas, 2015 m. antras ketvirtis**

- **Duomenų vagystės** – neteisėtai pasisavinti asmeniniai aukų duomenys, pavyzdžiui, slaptažodžiai, prisijungimo duomenys yra naudojami masiniams internetinių svetainių užkrėtimams. Tokiais būdais nusikaltėliai, kurie valdo botnet tinklą gauna tiesioginę finansinę naudą.

Tai toli gražu nėra baigtinis botnet tinklų panaudojimo sąrašas, tik išskirtos pagrindinės nusikalstamos veikos, su kuriomis yra susiduriama dažniausiai.

3. **Turinio nusikaltimai.**

Neteisėto turinio platinimas elektroninėje erdvėje yra labai paplitusi nusikaltimų rūšis (pornografinio turinio medžiagos, rasistinio ir kitokio pobūdžio diskriminacijos, šmeižto, grasinimų skleidimas yra didelė problema elektroninėje erdvėje).

4. **Nusikaltimai susiję su autorių teisių ir gretutinių teisių pažeidimais.**

Vieni iš labiausiai paplitusių nusikaltimų elektroninė erdvėje yra intelektinės nuosavybės pažeidimai. Tai galėtų būti neteisėtas intelektinių kūrinių, tokių kaip fotografijos, muzikos, literatūros darbų, filmų platinimas. Baudžiamuosiuose įstatymuose paminėta, kokios autorių teisės gali būti pažeidžiamos. Pažeistos gali būti autoriaus teisė viešai rodyti, atgaminti kūrinį.

Lietuvos kriminalinės policijos biuro Nusikaltimų elektroninėje erdvėje tyrimo valdybos pareigūnai siekiant kuo labiau išvengti elektroninių nusikaltimų galimybių rekomenduoja atnaujinti turimą operacinę sistemą, antivirusinę programinę įrangą bei kitas naudojamas programas. Taip pat, vartotojams rekomenduojama:

- „neatidarinėti įtartinų failų, nuorodų, gautų el. paštu;
- kilus abejonei, patikrinti failą šioje (https://www.virustotal.com) arba CERT.LT internetinėje svetainėje (https://www.cert.lt/antivirus). Dažnai antivirusinės programos atpažįsta kenksmingą kodą praėjus tik kelioms dienoms;
- nuolat kurti atsargines duomenų kopijas“ (Lietuvoje plinta pavojingas virusas: saugokite savo duomenis, 2015).

Pažangios interneto technologijos suteikia galimybes nusikaltėliams vykdyti kriminalinius tikslus. Kuo labiau tobulėja technologijos, tuo labiau tobulėja ir nusikaltimai. Dėka interneto globalumo, internete veikia organizuotos nusikalstamos grupuotės, kurias sudaro programišiai iš viso pasaulio.

1.3 Europos kibernetinio saugumo aktualumas

Gausus interneto vartotojų skaičius ir didelės gyvenimo dalies perkėlimas į elektroninę erdvę, kurioje atitinkamai išaugo ir nusikaltimų padaroma žala, paskatino Europos komisiją imtis su kibernetinį saugumą užtikrinančių priemonių.

„Kibernetiniu saugumu buvo stipriai susirūpinta jau 2001 metais, kuomet buvo pasirašyta Konvencija dėl kibernetinių nusikaltimų (Budapešto konvencija). Konvencija dėl

elektroninių nusikaltimų buvo pirmasis tarptautinis norminio pobūdžio dokumentas, skirtas spręsti nusikalstamų veikų kompiuteriniuose tinkluose problemas. Lietuva Konvenciją pasirašė 2003 m. birželio 23 d., o ratifikavo, 2004 m. kovo 18 d.“ (Kiškis, 2006). Šios konvencijos pagrindinis tikslas – siekti kuo didesnio narių bendradarbiavimo saugant tarptautinę bendruomenę nuo kibernetinių nusikaltimų. Svarbiausia yra bendros politikos formavimas per tinkamą reglamentavimą.

2003 m. gruodžio 13 d. Briuselyje Europos Taryba priėmė Europos saugumo strategiją (A Secure Europe in a Better World“, European Security Strategy, 2003). Dokumentas pavadintas „Saugi Europa geresniame pasaulyje“ yra trumpas, tačiau išsamus dokumentas, kuriame analizuojama ir nustatoma ES saugumo aplinka, nustatyti pagrindiniai saugumo iššūkiai bei aptartos vėlesnės politinės pasekmės. Šiame dokumente buvo išskirtos penkios pagrindinės grėsmės:

1. Terorizmas;
2. Didėjanti masinio naikinimo ginklų apimtis;
3. Regioniniai konfliktai;
4. Žlugančios valstybės;
5. Organizuotas nusikalstamumas.

2008 m. gruodžio 11 d. dėl pasikeitusios strateginės aplinkos buvo išleistas papildantis dokumentas – ataskaita dėl Europos saugumo strategijos įgyvendinimo „Saugumo užtikrinimas besikeičiančiame pasaulyje“ (Report on the Implementation of the European security Strategy, „Providing Security in a Changing World“, 2008). Šiame dokumente buvo išskirtos naujos grėsmės ES, tai – kibernetinio saugumas, energetinis saugumas ir klimato kaita.

2013 m. vasario 7 d. buvo paskelbta Europos Sąjungos kibernetinio saugumo strategija: atvira, saugi ir patikima kibernetinė erdvė. Ją paskelbė Europos Komisija ir Sąjungos vyriausioji įgaliotinė užsienio reikalams ir saugumo politikai. Strategijoje išdėstomi principai, pagal kuriuos reikėtų orientuoti kibernetinio saugumo politiką Europos Sąjungoje ir visame pasaulyje. Pagrindiniai principai, kuriais privaloma vadovautis vykdant kibernetinio saugumo politiką pagal ES kibernetinio saugumo strategiją yra šie:

1. **Pagrindinių žmogaus teisių, žodžio laisvės, asmens duomenų ir privatumo apsauga**. Veiksmingo kibernetinio saugumo pagrindas yra žmogaus teisės ir laisvės, kurios yra įtvirtintos Europos Sąjungos pagrindinių teisių chartijoje.
2. **Interneto prieiga visiems**. Piliečiams privalo būti užtikrinta neribota prieiga prie interneto ir reikalingos informacijos.

3. **Demokratiškas daugelio suinteresuotųjų šalių dalyvavimu grindžiamas valdymas.** Tiek valstybiniai, tiek ir komerciniai dariniai, kurie įsitraukę į kasdieninį interneto resursų valdymą dalyvauja skaitmeniniame pasaulyje.
4. **Bendra atsakomybė siekiant užtikrinti saugumą**. Tiek viešasis sektorius, tiek privačios įmonės, tiek individualūs vartotojai turi pripažinti šią bendrą atsakomybę ir imtis apsaugos priemonių siekiant sustiprinti kibernetinį saugumą.

ES kibernetinio saugumo strategijoje išskiriami penki strateginiai prioritetai:

- „Pasiekti kibernetinį atsparumą;
- Radikaliai sumažinti elektroninių nusikaltimų skaičių;
- Sukurti kibernetinės gynybos politiką ir pajėgumus, susijusius su bendra saugumo ir gynybos politika;
- Plėtoti pramonės ir technologinius išteklius kibernetiniam saugumui užtikrinti;
- Sukurti nuoseklią tarptautinę Europos Sąjungos kibernetinės erdvės politiką ir remti pagrindines ES vertybes“ (Europos Sąjungos kibernetinio saugumo strategija: atvira, saugi ir patikima kibernetinė erdvė, 2013).

ES kibernetinio saugumo strategija yra ES veiksmų planas, kaip galima būtų užkirsti kelią kibernetiniams incidentams bei kokių priemonių reikia imtis.

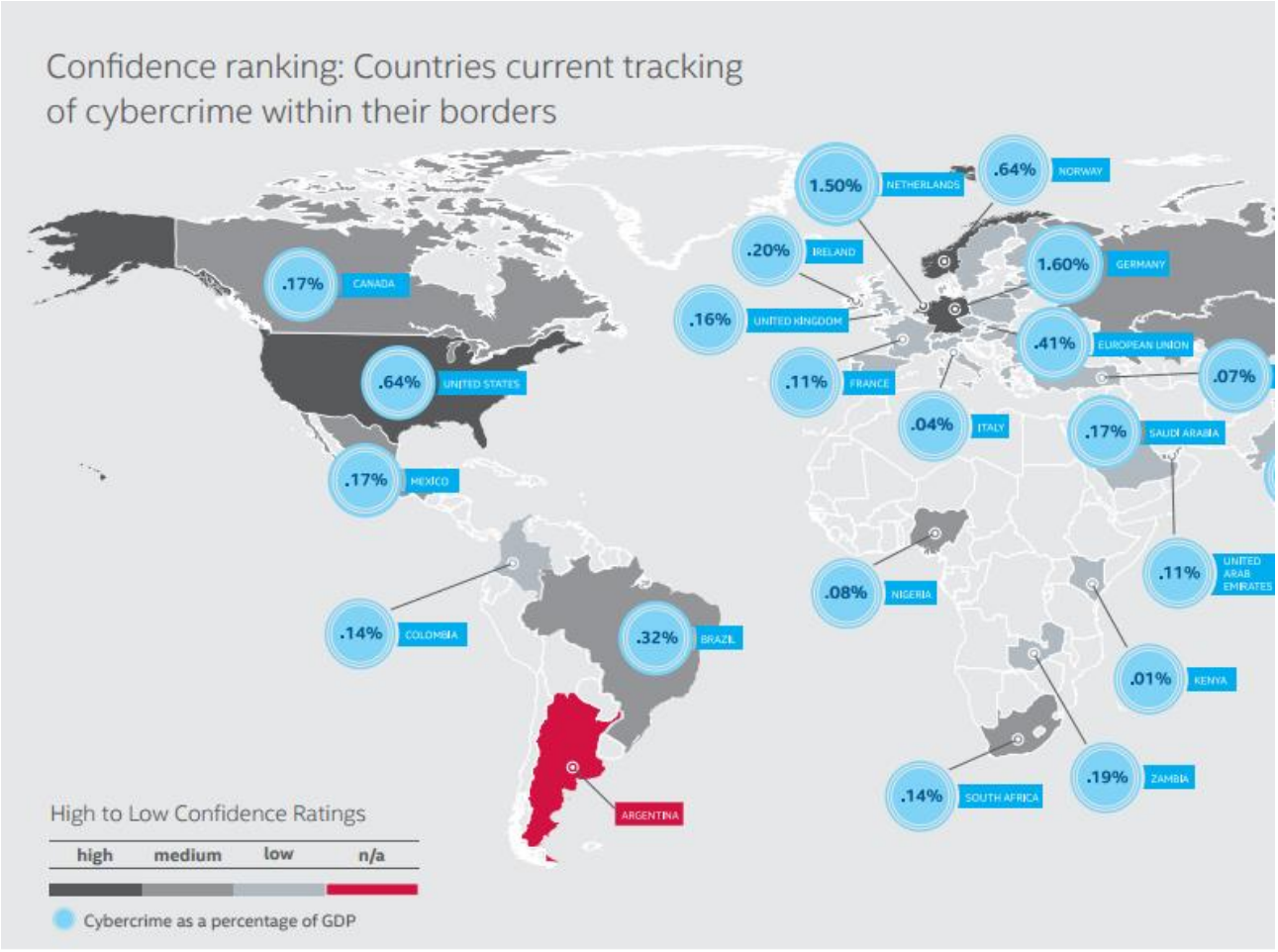
KIBERNETINIO SAUGUMO VALDYMO PASAULINĖS PATIRTIES ANALIZĖ

JAV 2005 – 2012 metais kompiuteriniai nusikaltėliai iš įvairių bankų pavogė daugiau nei 300 mln. JAV dolerių, tačiau ši suma jokiu būdu nėra baigtinė žalos suma, nes siekiant pinigus sugražinti, buvo sugaišta daugybė laiko ir išleista daug pinigų techninėms priemonėms. Bet kokie kibernetiniai nusikaltimai neigiamai veikia įmonių patikimumo reitingus bei finansiškai smukdo verslą į prarają.

UNOCD apskaičiavo, kad „tapatybės vagystė elektroninėje erdvėje yra pati pelningiausia elektroninių nusikaltimų forma. Per vienerius metus žala už tokius nusikaltimus siekia apie 1 milijardą JAV dolerių. Tuo tarpu sąnaudos siekiant nustatyti kaltininkus siekia 780 milijonų JAV dolerių per metus“ (Center for Strategic and International Studies & McAfee, 2013).

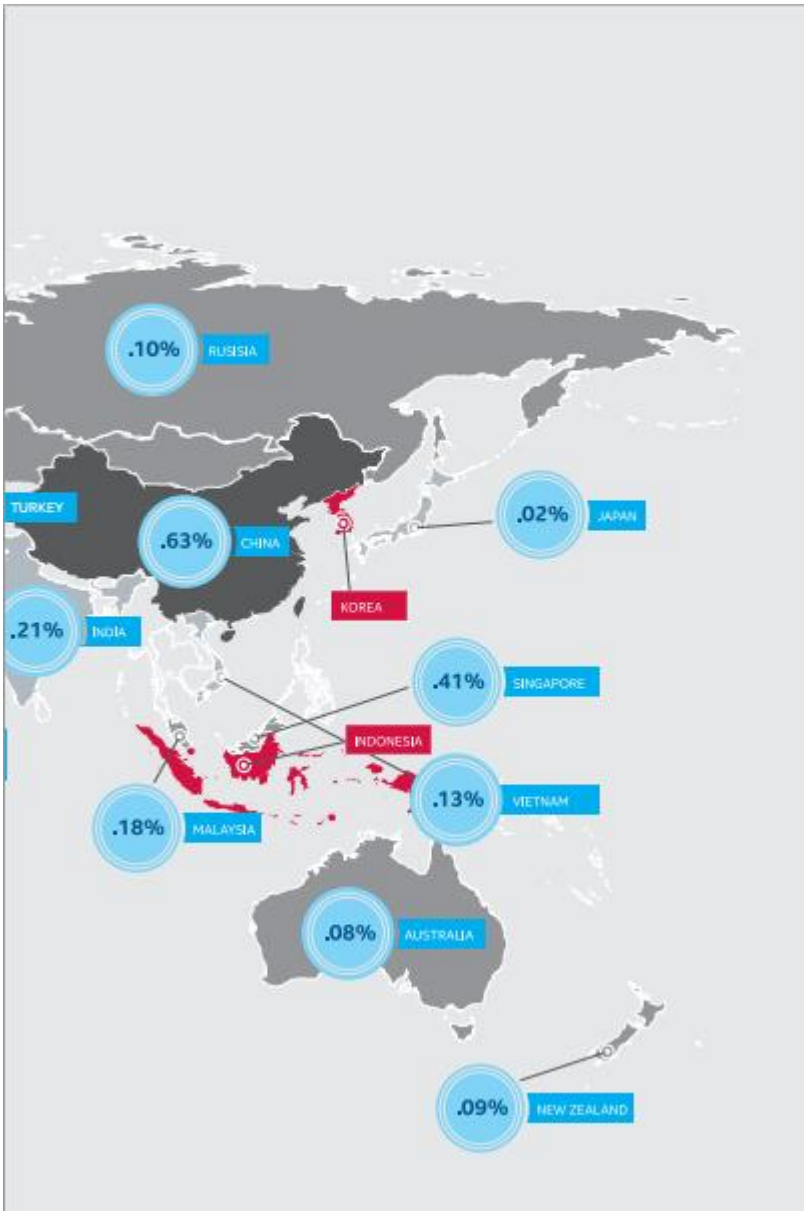
Kibernetinių nusikaltimų industrija yra auganti. Pelnas iš nusikaltimų palyginti labai didelis su rizika įkliūti teisėsaugai. „Prognozuojama, kad metinės išlaidos siekiant apsisaugoti nuo kibernetinių nusikaltimų pasaulio ekonomikai kainuoja daugiau nei 400 mlrd. JAV dolerių per metus. Optimistiškiausia suma būtų 375 mlrd. JAV dolerių, na, o maksimaliai žala galėtų siekti maždaug 575 mlrd. JAV dolerių per metus“ (Center for Strategic and International Studies & McAfee, 2014). Pateiktos sumos yra didesnės nei daugelio pasaulio valstybių nacionalinės metinės pajamos. Deja, bet daugelis valstybių bei verslo įmonių iki šiol rimtai neįvertina šių rodiklių grėsmės valstybių ekonomikoms. CERT- Australija duomenimis, tik 44 proc. įmonių, 2012 m. patyrusių kibernetinius incidentus pranešė apie tai atitinkamoms institucijoms. Tokia pati situacija, kai yra nepranešama apie kibernetinius incidentus Nyderlanduose.

2014 m. JAV kibernetinių nusikaltimų žala sudarė 0,64 proc. šalies BVP (Tarptautinio valiutos fondo duomenimis, JAV BVP 2014 metais siekė 17 049 mlrd. JAV dolerių), tuo tarpu Europoje, pagal kibernetinių incidentų žalą lyderė yra Vokietija, kurios elektroninių incidentų žala sudaro 1,6 proc. BVP (Pasaulio banko duomenimis, Vokietijos BVP 2014 metais siekė 3 852 mlrd. JAV dolerių).



Šaltinis: Center for Strategic and International Studies & McAfee report, „Net Losses Estimating the Global Cost of Cybercrime“, 2014.

Pav. 5 **Pasaulio valstybių kibernetinių nusikaltimų žalos proc. priklausomybė nuo valstybių BVP**



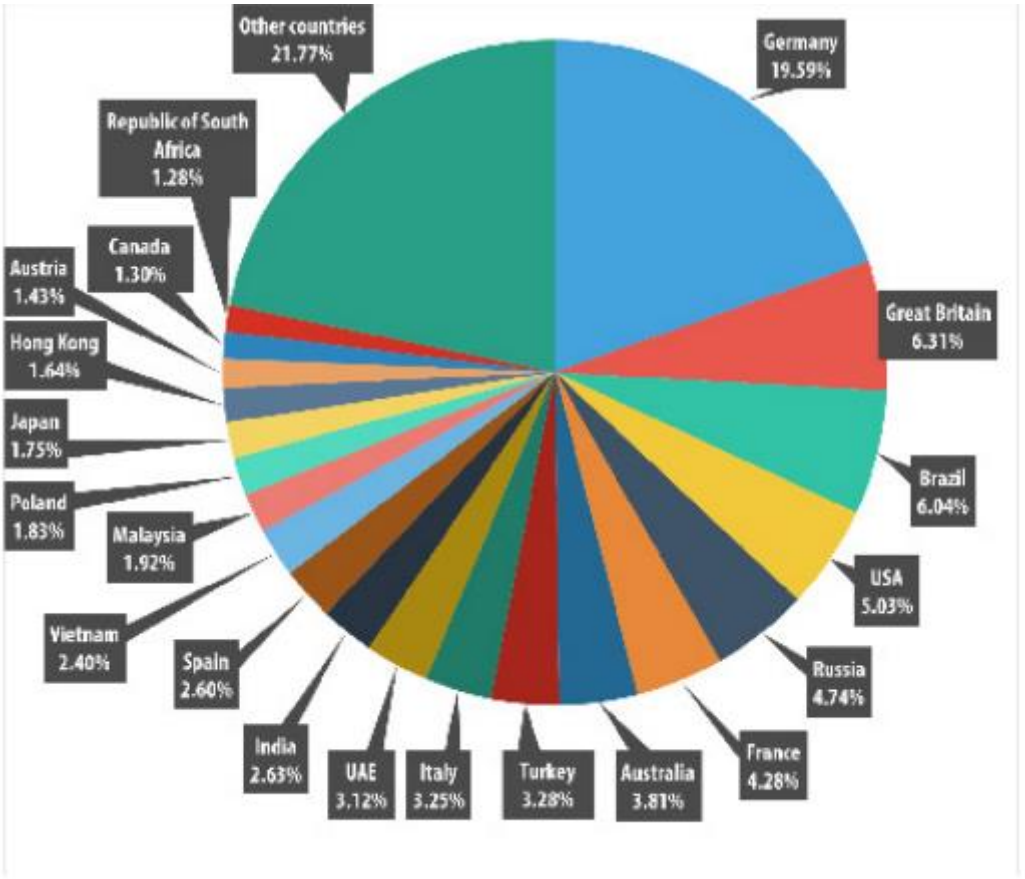
Šaltinis: Center for Strategic and International Studies & McAfee report, „Net Losses Estimating the Global Cost of Cybercrime“, 2014.

Pav. 6 **Pasaulio valstybių kibernetinių nusikaltimų žalos proc. priklausomybė nuo valstybių BVP**

Dėl kibernetinių incidentų, vidutiniškai valstybės praranda po 0,5 proc. jų metinio BVP. Paveiksle matyti, kad JAV, Europa ir Azija netenka daugiausiai pinigų lyginant su Afrika. Valstybių ekonominė situacija yra glaudžiai susijusi su kibernetiniu nusikalstamu – kuo valstybė yra turtingesnė (tuo tarpu ir jos kompanijos), tuo labiau ji traukia kibernetinius nusikaltėlius. Kuo turtingesnė valstybė, tuo didesnį pelną nusikaltėliams ji garantuoja, tačiau būtina paminėti ir tai, kad turtingos šalys turi finansinę galimybę investuoti į kibernetinę gynybą ir prevenciją. Kibernetinių incidentų mastui taip pat įtakos turi ir gerai išplėtota interneto infrastruktūra.

„Karspersky lab“ duomenimis, 2015 m. antrąjį ketvirtį, daugiausia kibernetinių nusikaltimų patyrusios šalys buvo Vokietija, Didžioji Britanija, Brazilija ir Jungtinės Amerikos

Valstijos. Tiek 2014 metais, tiek ir 2015 metais, Vokietija išlieka lyderė pagal elektroninių nusikaltimų skaičių pasaulyje.



Šaltinis: Karspersky Lab report, „Spam & Phishing in Q2 2015“.
https://securelist.com/files/2015/08/KL_Q2_2015_SPAM_REPORT_ENG.pdf.

Pav. 7 **Šalys, patyrusios kibernetinius nusikaltimus 2015 m. antrąjį ketvirtį**

1.4 Kibernetinio saugumo strategijos

Didėjanti kibernetinio saugumo grėsmė pastaraisiais metais lėmė tai, kad daugybė valstybių suskubo kurti ir plėtoti savo nacionalines kibernetinio saugumo strategijas. Pasak Europos Sąjungos tinklų ir informacijos saugumo agentūros ENISA, nacionalinė kibernetinio saugumo strategija yra veiksmų planas, kuriais siekiama pagerinti valstybės nacionalinių infrastruktūrų saugumą ir atsparumą. Tai dokumentas, nustatantis nacionalinius tikslus ir prioritetus, kurie turėtų būti pasiekti per tam tikrą laikotarpį.

Išsamiau bus analizuojamos ir tarpusavyje palyginamos Kanados (2010), Jungtinių Amerikos Valstijų (2011), Prancūzijos (2011), Vokietijos (2011), Čekijos (2011), Austrijos (2013) ir Naujosios Zelandijos (2011) kibernetinio saugumo strategijos. Bus lyginamos pagrindinės sąvokos, kylančio grėsmės, tikslai, pagrindiniai principai. Nors kiekvienos nacionalinio kibernetinio saugumo strategijos tikslas turėtų būti kibernetinių grėsmių mažinimo ar šalinimo sprendimai, egzistuoja skirtingi šalių pasirinkti taikymo metodai.

1.4.1 Kibernetinio saugumo sąvokos apibrėžimas skirtingų šalių strategijose

Skirtingų šalių kibernetinio saugumo strategijose *kibernetinis saugumas* apibrėžiamas skirtingai.

lentelė 1 Kibernetinio saugumo apibrėžimai skirtingų šalių strategijose

Šalis	Apibrėžimas	Kibernetinis saugumas tai:
Kanada	Aprašomojo pobūdžio	Tinkamo saugumo lygio užtikrinimas (kibernetinės atakos metu, t. y. tyčinio neteisėtos prisijungimo, naudojimo, valdymo ar sunaikinimo atveju) kurios metu naudojamasi elektroninės informacijos priemonėmis ir (arba) naudojant fizinę infrastruktūrą.
Jungtinės Amerikos Valstijos	Neišreikštas, bet numanomas	Pateiktas kaip „informacijos saugumas“
Prancūzija	Aiškus apibrėžimas	Informacijos sistema leidžianti pasipriešinti įvykiams, kurie gali pakenkti prieinamumui, vientisumui ar saugumui duomenų, kurie yra saugojami, apdorojami ar perduodami tarp informacijos ir ryšių sistemų.
Vokietija	Aiškus apibrėžimas	Globalaus kibernetinio saugumo tikslas yra IT saugumo rizikų sumažinimas iki priimtino lygio.
Austrija	Aiškus apibrėžimas	Terminas „kibernetinis saugumas“ reiškia infrastruktūrų saugumą kibernetinėje erdvėje, kurioje žmonės keičiasi duomenimis.
Čekija	Nepateikia apibrėžimo	-
Naujoji Zelandija	Aiškus apibrėžimas	Veikla, kuri padaro kibernetinę erdvę saugią nuo įsilaužimų, leidžia išlaikyki informacijos konfidencialumą, vientisumą ir prieinamumą nustatant įsilaužimus ir incidentus.

Sudaryta autoriaus pagal Kanados, JAV, Prancūzijos, Vokietijos, Austrijos, Čekijos ir Naujosios Zelandijos kibernetinio saugumo strategijas.

Penkios iš septynių šalių pateikia aiškius kibernetinio saugumo sąvokos apibrėžimus. Kanada kibernetinio saugumo sąvokai apibūdinti naudoja aprašomąjį tekstą (aprašą). Čekija nepateikia nei kibernetinio saugumo apibrėžimo nei aprašo. Gali būti, kad kai kurios valstybės skiria

dėmesį informacijos saugumo aspektams, o kai kurios kibernetinį saugumą laiko kaip būdą spręsti grėsmes kibernetinėje erdvėje.

Lietuvos Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011- 2019 metais programoje kibernetinio saugumo apibrėžimas nepateiktas, tačiau įvardinta, kad kibernetinis saugumas yra elektroninės informacijos saugos sinonimas. Tuo tarpu Lietuvos Respublikos kibernetinio saugumo įstatyme, kibernetinio saugumo sąvoka aiškiai apibrėžta tai – „visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti“ (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

Akivaizdu, kad vieningo apibrėžimo, kas yra kibernetinis saugumas tarp nagrinėjamų strategijų nėra.

1.4.2 Taikymo sričių analizė

Vokietijos kibernetinio saugumo strategijos teigia, kad kibernetinės grėsmės apima tik tuos informacijos ir ryšių objektus, kurie yra prijungti prie interneto. Kanados ir Naujosios Zelandijos strategijose teigiama, kad pagrindinis dėmesys turėtų būti skiriamas tik tiems informacijos ir komunikacijos objektams, kurie yra prijungti prie tinklo.

Deja, bet toks šių strategijų požiūris dėl taikymo srities gali lemti atsainų kibernetinio saugumo požiūrį į objektus, kurie tiesiogiai nėra prisijungę prie interneto.

lentelė 2 Valstybių strategijų palyginimas

	Kanada	**JAV**	**Prancūzija**	**Vokietija**	**Čekija**	**Austrija**	**Naujoji Zelandija**
Sukūrimo data	2010	2011	2011	2011	2011	2013	2011
Ar tai pirmoji strategija?	taip	Ne, pirmoji paskelbta 2003	taip	taip	taip	taip	taip
Taikymo sritis. Apima visas grėsmes susijusias su informacinėmis ir ryšių technologijomis (ICT)	Apima tik tas grėsmes, kurios kyla prie interneto prijungtoms sistemoms	Netiesiogiai apima visas sistemas	Apima visų sistemų grėsmes	Apima tik tas grėsmes, kurios kyla prie interneto prijungtoms sistemoms	Apima visų sistemų grėsmes	Apima visų sistemų grėsmes	Apima tik tas grėsmes, kurios kyla prie tinklo prijungtoms sistemoms
Sąsajos su kitomis strategijomis	Turi sąsajų su Nacionaline saugumo strategija (*First Defense Strategy, Canada*) ir	Turi sąsajų su Nacionaline saugumo strategija (*National Security*	Turi sąsajų su Nacionaline saugumo strategija (*French White*	Turi sąsajų su Nacionaline saugumo strategija (*Defense Policy*	Turi sąsajų su Nacionaline saugumo strategija (*Security Strategy of the Czech*	Turi sąsajų su Nacionaline saugumo strategija ir Kritinių infrastruktūr	Turi sąsajų su Nacionaline saugumo strategija (*New Zealand's National*

	Kritinių infrastruktūrų saugumo strategija (*Action Plan for Critical Infrastructure 2014-2017*)	*Strategy, 2015*)	*Paper. Defense and National security, 2013*)	*Guidelines, 2011*)	*Republic, 2015*)	ų saugumo programa	*Security System, 2011*)
Pagrindinės grupės, kurioms priskiriama kibernetinės grėsmės rizika	Nacionaliniam saugumui, kritinės infrastruktūroms objektams, ekonominei šalies gerovei, piliečių socialiniam gyvenimui, su šalies gynyba susijusiems objektams	Nacionaliniam saugumui, ekonominei šalies gerovei	Nacionaliniam saugumui, kritinės infrastruktūroms objektams	Kritinės infrastruktūroms objektams, ekonominei šalies gerovei	Nacionaliniam saugumui, kritinės infrastruktūroms objektams, ekonominei šalies gerovei, piliečių socialiniam gyvenimui.	Nacionaliniam saugumui	Nacionaliniam saugumui, kritinės infrastruktūroms objektams, ekonominei šalies gerovei
Pagrindinės kibernetinės grėsmės	Pavieniai nusikaltėlių ir nusikalstamų grupuočių veiksmai, šnipinėjimas, nusikalstamos veikos iš užsienio (kibernetinis karas), kibernetinis terorizmas	Šnipinėjimas, nusikalstamos veikos iš užsienio (kibernetinis karas), kibernetinis terorizmas; grėsmė gynybos pajėgumams, poveikis piliečių socialiniam gyvenimui	Pavieniai nusikaltėlių ir nusikalstamų grupuočių veiksmai, šnipinėjimas, nusikalstamos veikos iš užsienio (kibernetinis karas), kibernetinis terorizmas	Pavieniai nusikaltėlių ir nusikalstamų grupuočių veiksmai, šnipinėjimas, nusikalstamos veikos iš užsienio (kibernetinis karas), didelio masto kibernetinės atakos, globalizacijos stagnacija, informacijos ir ryšių technologijų (ICT) plėtros ir atitinkamo saugumo lygio neužtikrinimas	Pavieniai nusikaltėlių ir nusikalstamų grupuočių veiksmai, nusikalstamos veikos iš užsienio (kibernetinis karas), kibernetinis terorizmas	Pavieniai nusikaltėlių ir nusikalstamų grupuočių veiksmai, nusikalstamos veikos iš užsienio (kibernetinis karas), didelio masto kibernetinės atakos, kibernetinis terorizmas, sukčiavimas, tapatybės vagystės	Propaganda, pavieniai nusikaltėlių ir nusikalstamų grupuočių veiksmai, šnipinėjimas, nusikalstamos veikos iš užsienio (kibernetinis karas), kibernetinis terorizmas

Sudaryta autoriaus pagal Kanados, JAV, Prancūzijos, Vokietijos, Austrijos, Čekijos ir Naujosios Zelandijos kibernetinio saugumo strategijas ir (Luiijf, H. A. M et al., 2013).

Dauguma pasirinktų strategijų buvo paskelbtos pirmą kartą. Jungtinės Amerikos Valstijos kibernetinio saugumo strategija pirmą kartą buvo paskelbta 2003 metais, tuomet kibernetinis saugumo problema dar nebuvo tokia opi kaip šiomis dienomis. 2011 metais JAV atnaujino savo kibernetinio saugumo strategiją ją papildydama.

1.4.3 Kibernetinio saugumo strategijų sąsajos su kitomis strategijomis

Visos nagrinėjamos strategijos buvo kuriamos remiantis šalių Nacionalinio saugumo strategijų pagrindu. Nors kritinių infrastruktūrų saugumas akcentuojamas daugumoje strategijų, tik Kanados ir Austrijos strategijos vadovaujasi Kritinių infrastruktūrų saugumo užtikrinimo principais.

Dauguma strategijų teigia, kad kibernetines grėsmes turi neigiamą įtaką šalies ekonominei gerovei. Europos Sąjungos valstybės ypatingą dėmesį atkreipia į tai, kad reikalingas glaudesnis Europos Sąjungos šalių narių bendradarbiavimas siekiant pažaboti kibernetinius nusikaltimais, bei kritinės svarbos infrastruktūros apsaugą. „Europos Sąjungos dokumentuose pažymima, kad „ypatingos svarbos informacinės infrastruktūros objektai gyvybiškai būtini ES ekonomikos ir visuomenės plėtrai“, o informacinių technologijų ir interneto plėtra (skvarba) gerina ekonominius rodiklius, užtikrina visuomenės socialinės gerovės augimą bei piliečių gyvenimo kokybę“ (Štitilis, 2013).

ES šalys siekiant vieningo kibernetinio saugumo užtikrinimo turėtų sieti savo nacionalines kibernetinio saugumo strategijas su ES kibernetinio saugumo strategija. ES kibernetinio saugumo strategija yra išsamus strateginis dokumentas, kuriame reglamentuojami esminiai principai, tikslai, kibernetinio saugumo užtikrinimo lygiai bei valstybių narių ir Komisijos bendradarbiavimo mechanizmas.

1.4.4 Pagrindinių grėsmių ir jų sukėlėjų analizė

Didžioji dauguma šalių kaip pagrindines grėsmes kibernetinėje erdvėje išskyrė pavienių nusikaltėlių ir nusikalstamų grupuočių veiksmus, šnipinėjimą virtualioje erdvėje, nusikalstamas veikas iš užsienio (kibernetinis karas), kibernetinį terorizmą. Kibernetinių atakų grėsmė ir kova prieš jas yra įvardijama kaip prioritetas visose pasirinktų šalių Nacionalinio saugumo strategijose. Kanada įvardijo kibernetinio pavojas grėsmę šalies gynybos pajėgumams. Nepaisant to, kad vienas iš Prancūzijos strategijoje nurodytų tikslų yra įgyti pasaulinę galią kibernetinės gynybos srityje, ši šalis neįvardijo gynybos pajėgumams kylančių kibernetinių grėsmių kaip vienų iš pagrindinių. Vokietija paminėjo globalizacijos stagnacijos riziką, kas būtų nepalanku šaliai ekonominiu požiūriu. Ši grėsmė gali padaryti neigiamą įtaką Vokietijos visuomenei informacijos ir ryšių technologijų kontekste (pvz.: socialiniams santykiams virtualioje erdvėje). Grėsmę piliečių socialiniam gyvenimui paminėjo ir Kanada.

Taigi, dauguma valstybių pagrindines kibernetinėje erdvėje esančias grėsmes mato kaip elektroninių nusikaltėlių veiksmus, šnipinėjimą virtualioje erdvėje, tačiau tik nedidelė dalis šalių prie grėsmių priskiria pavojų nacionaliniams gynybos pajėgumams, ekonomikos gerovei bei piliečių socialinio gyvenimo saugumui.

Visos valstybės kaip grėsmių sukėlėjus įvardijo pavienius nusikaltėlius, nusikalstamas grupuotes. Taip pat, visos šalys, išskyrus Naująją Zelandiją kaip potencialius grėsmių sukėlėjus paminėjo priešiškai nusiteikusius nusikaltėlius iš užsienio valstybių, kurie gali sukelti pvz.: kibernetinį karą puolamoje šalyje. Visos tautos kaip grėsmę keliančius objektus paminėjo kibernetinius teroristus, kurie potencialiai gali padaryti žalą šalių kritinėms infrastruktūroms. Vokietija kaip didelę grėsmę išskiria didelio masto kibernetines atakas prieš šalies kritinės infrastruktūros objektus, kurias atlieka kibernetiniai teroristai. Taip pat ši šalis išskiria dar vieną labai svarbų aspektą tai – informacijos ir ryšių technologijų (ICT) plėtros ir atitinkamo saugumo lygio užtikrinimo problemą.

1.4.5 Strateginių tikslų analizė

Kiekviena valstybės strategija pateikia savo strateginius tikslus. Jie pateikti lentelėje. Visų strategijų tikslai apima tris pagrindines sritis: nacionalinį saugumą, kritinių infrastruktūrų ir piliečių apsaugą. Visos strategijos, išskyrus Austrijos strategiją, kaip strateginį tikslą išskiria kritinės infrastruktūros objektų apsaugą, tačiau galima numanyti, kad Austrijos strateginis tikslas, kuris apsaugotų kritinės infrastruktūros objektus yra įvardintas kaip tikslas padaryti informacinių ir ryšių technologijų (ICT) infrastruktūras saugios ir atsparios grėsmėms.

lentelė 3 Pagrindiniai valstybių kibernetinio saugumo strategijų tikslai

Valstybė	Strateginiai tikslai
Kanada	1. Nacionalinių (vyriausybinių) sistemų apsauga; 2. Privataus ir vyriausybinio sektoriaus partnerystė siekiant apsaugoti nevyriausybines sistemas; 3. Užtikrinamas Kanados piliečių saugumas virtualioje erdvėje.
JAV	1. Užkirsti kelią kibernetinėms atakoms nukreiptoms prieš JAV kritinės infrastruktūros objektus; 2. Sumažinti nacionalinį pažeidžiamumą nuo kibernetinių atakų; 3. Kuo labiau sumažinti kibernetinių atakų padarinių žalą ir atkūrimo laiką.
Prancūzija	1. Turėti pasaulinę galią kibernetinio saugumo srityje; 2. Užtikrinti Prancūzijos laisvę priimant sprendimus susijusius su nacionalinės informacijos saugumu; 3. Užtikrinti kibernetinį saugumą nacionaliniuose kritinės svarbos infrastruktūros objektuose; 4. Užtikrinti saugią kibernetinę aplinką
Vokietija	1. Ypatingos svarbos informacinės infrastruktūros objektų apsauga; 2. IT sistemų saugumas Vokietijoje; 3. IT saugumo stiprinimas viešajame sektoriuje; 4. Nacionalinis Kibernetinio Reagavimo Centras; 5. Nacionalinė Kibernetinio Saugumo Taryba; 6. Veiksminga nusikalstamumo kontrolė kibernetinė erdvėje;

	7. Efektyvūs suderinti veiksmai siekiant užtikrinti kibernetinį saugumą Europoje ir visame pasaulyje; 8. Patikimų informacinių technologijų naudojimas; 9. Federalinės valdžios personalo plėtra; 10. Priemonės, skirtos reaguoti į kibernetines atakas.
Čekija	1. Užtikrinti saugią ir patikimą aplinką, kuri leistų naudotis skaitmeninių technologijų teikiamomis galimybėmis.
Austrija	1. Duomenų prieinamumas, patikimumas ir konfidencialumas gali būti užtikrintas tik saugioje ir patikimoje elektroninėje erdvėje. Virtuali erdvė privalo būti atspari rizikos veiksniams, atakoms, turi prisitaikyti prie pakitusios aplinkos; 2. Nacionaliniu požiūriu, kompetentingos Austrijos federalinės ministerijos užtikrins, kad informacinių ir ryšių technologijų (ICT) infrastruktūros būtų saugios ir atsparios grėsmėms. Užtikrintas viešojo ir privataus sektoriaus bendradarbiavimas; 3. "Kibernetinis saugumas", kaip turtas, yra saugomas Austrijos valdžios institucijų; 4. Teikiant informaciją apie kibernetinio saugumo svarbą, Austrijoje yra formuojama "kibernetinio saugumo kultūra"; 5. Austrija tampa patraukli verslo vieta investuotojams; 6. Austrija atlieka svarbų vaidmenį vykdant tarptautinį bendradarbiavimą Europos ir pasaulio mastu, ypač keičiantis informacija bei patirtimi formuojant tarptautines strategijas; 7. Stiprinama ir plėtojama Austrijos e-valdžios apsauga; 8. Bus apsaugotas visų Austrijos įmonių naudojamų programų vientisumas, o taip pat, užtikrinama asmens duomenų privatumo apsauga įmonių klientams. Glaudus ir sistemingas bendradarbiavimas tarp įmonių vaidina lemiamą vaidmenį šiame procese; 9. Austrijos gyventojai privalo žinoti savo asmeninę atsakomybę elektroninėje erdvėje. Visi piliečiai privalo naudotis elektronine erdve deramai, būti atsakingi už savo veiklą naudojantis internetu.
Naujoji Zelandija	1. Didinti informuotumą ir saugumą kibernetinėje erdvėje privatiems asmenims ir mažoms įmonėms; 2. Apsaugoti vyriausybines sistemas; 3. Tarpusavio bendradarbiavimo pagalba užtikrinti kibernetinį saugumą kritinės infrastruktūros objektams ir kitoms verslo įmonėms.

Sudaryta autoriaus pagal Kanados, JAV, Prancūzijos, Vokietijos, Austrijos, Čekijos ir Naujosios Zelandijos kibernetinio saugumo strategijas ir (Luiijf, H. A. M et al., 2013).

Kaip svarbų strateginį tikslą Kanada, Vokietija, Prancūzija, Austrija ir Naujoji Zelandija iškelia glaudų tarpusavio bendradarbiavimą tiek nacionaliniu, tiek ir tarptautiniu lygmeniu.

Svarbią vietą Naujosios Zelandijos ir Austrijos strategija skiria visuomenės informavimo sričiai pastarosios tikslas šalyje formuoti „kibernetinio saugumo kultūrą".

Prancūzija siekdama išlaikyti savo strateginę nepriklausomybę iš kitų strategijų išsiskiria tikslu įgyti pasaulinę galią kibernetinio saugumo srityje.

Visos išvardintos strategijos kaip svarbų tikslą įvardija valstybių piliečių apsaugą kibernetinėje erdvėje, kuri užtikrintų socialinę ir ekonominę gerovę.

1.4.6 Kibernetinių saugumo strategijų principai

Keturios iš septynių analizuojamų strategijų pateikia pagrindinius kibernetinio saugumo įgyvendinimo principus. Kanada, Prancūzija ir Naujoji Zelandija pagrindinių principų strategijoje neišskiria. Kanada savo kibernetinio saugumo strategijoje teigia, kad trys iš artimiausių jos saugumo ir žvalgybos partnerių t. y. JAV, Jungtinė Karalystė ir Austrija neseniai išleido savo strateginius planus kaip užtikrinti saugią kibernetinę erdvę. Daugelis iš pagrindinių principų ir veiklos prioritetų išdėstyti partnerių ataskaitose primena ir Kanados kibernetinio saugumo užtikrinimo principus.

lentelė 4 Pagrindiniai valstybių strategijų kibernetinio saugumo principai

Valstybė	Strateginiai principai
Kanada	Nepateikta.
JAV	Turi būti apsaugotos visuomenės privatumas ir pilietinės teisės ir laisvės.
Prancūzija	Nepateikta.
Vokietija	Visos suinteresuotosios šalys privalo bendradarbiauti ir kartu siekti tikslų. Suinteresuotosios šalys vykdydamos užduotis turi vadovautis tarptautinėmis elgesio taisyklėmis, normomis ir standartais.
Čekija	1. Tvirtai laikytis demokratinės visuomenės principų ir tinkamai atsižvelgti į piliečių, verslo ir viešojo sektoriaus interesus; 2. Užtikrinti pakankamai saugias kibernetinio saugumo priemones siekiant apsaugoti ir garantuoti nacionalinį saugumą. Gerbti piliečių privatumą, pagrindines teises ir užtikrinti laisvą prieigą prie informacijos; 3. Užtikrinti subalansuotas nacionalinio kibernetinio saugumo priemones, kurios užtikrintų saugumą nevaržant pagrindinių piliečių teisių ir laisvių.
Austrija	1. Teisės aktų laikymasis; 2. Subsidiarumas;

	3. Savireguliacija; 4. Proporcingumas.
Naujoji Zelandija	Nepateikta.

Sudaryta autoriaus pagal Kanados, JAV, Prancūzijos, Vokietijos, Austrijos, Čekijos ir Naujosios Zelandijos kibernetinio saugumo strategijas ir (Luiijf, H. A. M et al., 2013).

Visos šalys, kurios savo strategijose išdėstė principus, vienbalsiai pasisako už pagrindinių piliečių teisių ir laisvių užtikrinimo, privatumo ir demokratinės visuomenės principų svarbą.

1.4.7 Kibernetinio saugumo strategijų apibendrinimas

Remiantis Prancūzijos strategija, nacionalinės valdžios institucijos ir krizių valdymo subjektai yra atsakingi už išteklių, kurie užtikrina jų bendradarbiavimą, buvimą. Privalo būti užtikrintas informacijos konfidencialumo lygis informacijos dalijimosi proceso metu. Tam tikslui pasiekti privalo būti naudojami atitinkami apsaugos produktai ir metodai. Taip pat privalo būti garantuotas kritinių infrastruktūrų saugumas bendradarbiaujant su atitinkamos įrangos gamintojais ir operatoriais. Siekiant užtikrinti viešojo ir privataus sektoriaus subjektų bei piliečių saugumą visos paslaugos privalo veikti pavyzdingai ir pagerinti esamų informacinių sistemų ir duomenų apsaugą.

Esminė JAV strategijos dalis yra viešojo ir privataus sektoriaus bendradarbiavimas. JAV kibernetinio saugumo strategija išskiria aktyvų bendradarbiavimą su kibernetines paslaugas teikiamomis bendrovėmis. Vyriausybės tikslas – pramonės bendradarbiavimas, užtikrinantis saugumą kibernetinėje erdvėje, nes infrastruktūros pardavėjai ir operatoriai teikia galimybes, kurios paprastai neatitinka vyriausybės pagrindinių kompetencijų bei galimybių. Kibernetines paslaugas teikiančios bendrovės gali valstybei padėti per:

- Ekspertų žinias apie tinklus, sistemas, priemones ir t.t.;
- Reagavimo į incidentus žinias ir patirtį;
- Gebėjimą kurti naujus produktus padėsiančius užtikrinti kibernetinį saugumą;
- Greitą interneto ir jo paslaugų projektavimą, diegimą, eksploatavimą, administravimą ir priežiūrą.

Privatus sektorius taip pat turi naudos iš viešojo sektoriaus:

- Valstybė turi išteklių pasiūlyti operatoriams tikslios informacijos apie kritinės infrastruktūros objektų grėsmes;
- Vyriausybė turi teisines priemones ir siekdama sukurti tokią aplinką, kuri skatintų visas įmones investuoti į kibernetinio saugumo užtikrinimą, gali padidinti nacionalinį saugumą;
- Vyriausybė gali remti mokslinius tyrimus siekiant apsaugoti elektroninę erdvę;

Apibendrinant, valstybė privalo užtikrinti vadovavimą viešojo ir privataus sektoriaus bendradarbiavimui skatindama dalintis informacija bei patirtimis. Privatus sektorius turi

kompetencijas tobulinti saugumo procesus siekiant valstybės iškeltų kibernetinio saugumo tikslų. Svarbu, kad vykdant procesus būtų užtikrintas duomenų saugumas bei nustatytos šalių atsakomybės.

Kanados strategija remiasi trimis pagrindiniais aspektais: vyriausybinių infrastruktūrų saugumo, partnerystės tarp viešojo, privataus sektorių ir kritinės infrastruktūros subjektų bei piliečių saugumo užtikrinimo virtualioje erdvėje. Kalbant apie pirmąją sritį – tam, kad būtų užtikrintas vyriausybinių infrastruktūrų saugumas būtina nustatyti aiškias pareigas ir atsakomybes, tam, kad būtų sustiprinta nacionalinių sistemų apsauga, o taip pat privalo būti formuojamas teisingas kibernetinių grėsmių suvokimas. Partnerystė tarp viešojo, privataus sektorių ir kritinės infrastruktūros subjektų yra svarbi, todėl vyriausybė yra pasiruošusi remti bendradarbiavimo iniciatyvas. Kanados piliečių saugumo užtikrinimas virtualioje erdvėje apima kovas su elektroniniais nusikaltimais bei saugios kibernetinės erdvės užtikrinimą norint išsaugoti piliečių privatumą.

Vokietija pagrindinį dėmesį skiria kibernetinių atakų prevencijai, o taip pat kritinių infrastruktūrų saugumo užtikrinimui. Šiuo tikslu bus sustiprinta IT sistemų apsauga viešajame sektoriuje. Vokietijos nuomone, Valstybinės valdžios institucijos privalo būti kaip pavyzdys ir demonstruoti duomenų saugumo svarbą. Tam yra svarbus operatyvinis bendradarbiavimas su CERT (kompiuterinių incidentų tyrimų tarnyba; angl. *computer emergency response teams*). Kaip ir dauguma kitų strategijų Vokietija akcentuoja tarpusavio bendradarbiavimą ir dalijimąsi gerąja praktika.

Čekijos kibernetinio saugumo strategijos esminiai tikslai apima apsaugą nuo grėsmių, kurios veikia informacijos ir ryšių (ICT) infrastruktūras, o taip pat grėsmių pasekmių mažinimą. Strategija kaip prioritetą iškelia laisvą prieigą prie elektroninių paslaugų, duomenų vientisumo ir konfidencialumo užtikrinimą.

Naujosios Zelandijos strategijos tikslas – valstybės atsakas į kasdien augančią kibernetinio saugumo grėsmę. Strategija pabrėžia vyriausybės, valstybinių ir privačių įmonių bei piliečių iniciatyvos svarbą siekiant apsaugoti virtualios erdvės saugumą. Naujosios Zelandijos tikslas yra didinti supratimą apie kibernetinį saugumą tarp piliečių ir įmonių, gerinti saugumo padėtį valdžios lygmenyje bei plėtoti strateginius santykius siekiant apsaugoti kritines infrastruktūros subjektus ir kitas įmones. Vyriausybė kreipėsi į platų suinteresuotųjų šalių ratą (pramonės, akademinės bendruomenės subjektus, privatų sektorių ir t.t.) siūlydama partnerystę siekiant bendro tikslo – saugios kibernetinės aplinkos. Tarptautiniu mastu, Naujoji Zelandija veiksmingai prisideda prie vykdomų kibernetinio saugumo iniciatyvų remdama šalių tarpusavio bendradarbiavimo svarbą.

Austrijos kibernetinio saugumo strategija yra išsamus dokumentas, kuriame tiksliai apibrėžta kibernetinio saugumo užtikrinimo koncepcija, kaip būtų galima apsaugoti elektroninę erdvę nesuvaržant Austrijos piliečių teisių. Priemonių, kurios išsamiai aptartos strategijoje tikslas yra užtikrinti Austrijos valstybinių ir ne valstybinių infrastruktūrų sklandų veikimą ir nepertraukiamą

elektroninių paslaugų tiekimą. Išskirtas svarbus aspektas – „kibernetinio saugumo kultūros“ formavimas, t. y. visuomenės informavimas ir švietimas apie grėsmes virtualioje erdvėje ir jų prevenciją.

Apibendrinant visas strategijas penkios iš septynių šalių pateikia aiškius kibernetinio saugumo sąvokos apibrėžimus. Tam kad nekiltų nesklandumų bendradarbiaujant tarptautiniu lygiu būtinas tarptautiniu mastu pripažintas ir suderintas kibernetinio saugumo apibrėžimas.

Dauguma strategijų pripažįsta, visuomenės informuotumo poreikį bei teisingą valstybių piliečių požiūrio formavimą į kibernetinį saugumą, tačiau kaip strateginį tikslą „kibernetinio saugumo kultūros“ formavimą ir piliečių atsakomybės stiprinimą išskiria tik Austrija.

Nuolat besivystančioje kibernetinėje erdvėje kyla ir vis didesnis grėsmių pavojus, todėl būtina formuojant kibernetinio saugumo strategijas atsižvelgti į šių dienų technologines aktualijas ir užtikrinti, kad prevencinės priemonės yra adekvačios kylančioms grėsmėms. Kadangi, kibernetinė erdvė yra visuotinė, visos šalys privalo bendradarbiauti ne tik nacionaliniu (viešojo ir privataus bendradarbiavimo principas), tačiau ir tarptautiniu lygmeniu. Europos Sąjungos valstybės ypatingą dėmesį atkreipia į tai, kad reikalingas glaudesnis Europos Sąjungos šalių narių bendradarbiavimas siekiant pažaboti kibernetinius nusikaltimais.

Apibendrinant visų valstybių kibernetinio saugumo strategijas, pastebima, kad visos valstybės kelia panašius tikslus, susijusius su tarpusavio bendradarbiavimu tiek nacionaliniu, tiek tarptautiniu lygiu taip pat akcentuojamas informacijos keitimasis ir geroji praktika. Išskirti pagrindiniai tikslai – kovoti su elektroniniais nusikaltimais bei gerinti atsparumą kibernetiniams incidentams, gilinti kibernetinio saugumo žinias bei stiprinti pajėgumus užtikrinant elektroninės informacijos saugumą. Taip pat, strategijose akcentuojami kritinės infrastruktūros apsaugos, visuomenės informavimo, informacinių technologijų stiprinimo viešajame sektoriuje uždaviniai kaip esminiai aspektai.

Tam, kad kibernetiniai nusikaltimai būtų suvaldomi visuotiniu (tarptautiniu) lygiu būtinas bendras valstybių požiūris į kibernetinį saugumą. ES narės turėtų stengtis suvienodinti savo strateginius tikslus, principus, prioritetus ir veiklos sritis, tam, kad būtų formuojamas vieningas suvokimas ir taip būtų lengviau siekti bendro tikslo. ES šalys atsižvigdamos į 2013 metais išleistą ES kibernetinio saugumo strategiją galėtų ją panaudoti kaip gaires formuojant savo nacionalines kibernetinio saugumo strategijas.

1.4.8 Veiksniai darantys įtaką kibernetinių nusikaltimų mastui

Vienoms valstybėms kur kas geriau sekasi pažaboti kibernetinius nusikaltimus, nei kitoms. Kyla klausimas – kas tai lemia? Iš valstybių, kurių strategijos buvo analizuotos išsiskiria dvi ES šalys, kurios pagal kibernetinių nusikaltimų statistiką (žiūrėti Pav. 7) stipriai skiriasi viena nuo

kitos. Tai - Vokietija ir Austrija, kurių kibernetinių nusikaltimų skirtumai kelia klausimą, kodėl tiek kultūrine, tiek ekonomine prasme panašių šalių padėtis tokia skirtinga elektroninių nusikaltimų srityje.

Vokietija – didžiausia pagal gyventojų skaičių Europos šalis (~81,8 mln. gyv.). Pagal BVP dydį – ketvirta pasaulyje ir yra laikoma viena turtingiausių ir ekonomiškai pajėgiausių šalių pasaulyje, viena iš Europos Sąjungos steigėjų. Vokietijos ekonomika yra didžiausia Europoje ir ketvirta pagal nominalųjį BVP pasaulyje.

Center for Strategic and International Studies & McAfee ataskaitos duomenimis 2014 m. Europoje, pagal kibernetinių incidentų žalą lyderė yra Vokietija, kurios elektroninių incidentų žala sudaro 1,6 proc. BVP (Pasaulio banko duomenimis, Vokietijos BVP 2014 metais siekė 3 852 mlrd. JAV dolerių, BVP vienam gyventojui 46 268 tūkst. JAV dolerių).

„Karspersky lab“ duomenimis, 2015 m. antrąjį ketvirtį, daugiausia kibernetinių nusikaltimų patyrusios šalys buvo Vokietija, Didžioji Britanija, Brazilija ir Jungtinės Amerikos Valstijos. Tiek 2014 metais, tiek ir 2015 metais, Vokietija išlieka lyderė pagal elektroninių nusikaltimų skaičių pasaulyje.

Tuo tarpu, „Karspersky lab“ duomenimis, Austrija 2015 m. antrąjį ketvirtį elektroninių nusikaltimų, lyginant su Vokietija) patyrė labai mažai. Tiek Vokietija, tiek Austrija yra labai gimininges šalys. Austrijos ekonomika apibūdinama kaip socialinė rinkos ekonomika, turinti panašią struktūrą kaip ir Vokietijos ekonomika. Šalyje yra labai aukštas gyvenimo lygis. Šalis yra viena iš 12 turtingiausių šalių pasaulyje. Pasaulio banko duomenimis, BVP 436 mln. JAV dolerių (išreiškus BVP vienam gyventojui 50 546 tūkst. JAV dolerių).

Toliau darbe bus išsamiai analizuojamos ir lyginamos šių dviejų ES šalių strategijos – strateginiai tikslai, saugumo principai, prioritetai, pagrindinės veiklos kryptys ir planuojami veiksmai, siekiant atsakyti į klausimą, kas gi lemia tokį didelį kontrastą tarp šių šalių kibernetinių incidentų skaičiaus.

1.5 Vokietijos kibernetinio saugumo strategija

Dėl vis didėjančios grėsmės elektroninėje infrastruktūroje, Vokietijos Vyriausybė parengė kibernetinio saugumo strategiją (Cyber Security Strategy for Germany, 2011), kuri buvo išleista 2011 m. vasario mėnesį ir kurios pasiūlymu buvo įsteigtas *Nacionalinis Kibernetinio Saugumo Reagavimo Centras* ir *Nacionalinė Kibernetinio Saugumo Taryba*. Vokietijoje visi socialinių ir ekonominio sektoriaus vartotojai naudojasi elektroninės erdvės teikiamomis galimybės. Kritiškai svarbios infrastruktūros, verslo subjektai ir paprasti piliečiai yra priklausomi nuo interneto ir vertina jo patikimumą. Blogai veikiantys IT produktai bei jų komponentai, kibernetinės atakos gali

turėti didelį neigiamą poveikį technologijų, verslo ir administravimo srityje bei visame Vokietijos socialiniame gyvenime. Kibernetinės erdvės prieinamumo, integralumo, autentiškumo ir konfidencialumo užtikrinimas tapo vienu didžiausių 21 amžiaus uždavinių tiek Vokietijoje, tiek ir visame pasaulyje.

Pagrindiniai Vokietijos kibernetinio saugumo strategijos principai

Vokietijos Federacinės Vyriausybės siekis yra užtikrinti saugią kibernetinę erdvę, kas garantuotų ekonominę ir socialinę gerovę Vokietijoje. Saugumas būtų užtikrintas nevaržant kibernetinės erdvės naudojimo. Būtinas saugumo lygis, siekiant apsaugoti informacijos ir tinklų duomenų saugumą t. y. vientisumą, autentiškumą ir konfidencialumą, būtų pasiektas naudojantis nacionalinėmis ir tarptautinėmis saugumo priemonėmis.

Kibernetinio saugumo strategija daugiausia dėmesio skiria civiliniams metodams ir priemonėms. Šie metodai papildo priemones, kurių ėmėsi Bundeswehr (Vokietijos kariuomenė), siekdama apsaugoti savo pajėgumus. Visa tai apima bendradarbiavimą su Europos Sąjunga, NATO, G8, ESBO ir kitomis tarptautinėmis organizacijomis. Pagrindinis siekis yra užtikrinti darnią tarptautinę kibernetinę erdvę.

Strateginiai tikslai ir priemonės

Remiantis kibernetinio saugumo strategija, Vokietijos federalinė vyriausybė pasitelkia priemones, siekdama išvengti iškilusių grėsmių. Vokietijos federalinė vyriausybė konkrečiai sutelkia dėmesį į dešimt strateginių krypčių:

1. **Ypatingos svarbos informacinės infrastruktūros objektų apsauga**

Ypatingos svarbos informacinės infrastruktūros objektų apsauga yra svarbiausia kibernetinio saugumo užtikrinimo dalis. Pasak Vokietijos Nacionalinio kibernetinio saugumo tarybos, tam svarbus glaudus viešojo ir privataus sektoriaus bendradarbiavimas su Vokietijos Federacine Vyriausybe, kuris privalo būti pagrįstas intensyviais informacijos mainais.

Įvardintas „glaudus viešojo ir privataus sektoriaus bendradarbiavimas“, tačiau neįvardintos konkrečios priemonės ir veiksmai, kuriais šis tikslas bus pasiektas. Pabrėžiama tik tikslo svarba.

2. **IT sistemų saugumas Vokietijoje**

Svarbu užtikrinti IT sistemų, kuriomis naudojasi piliečiai bei mažos įmonės saugumą. Tai gali būti pasiekta tik tuo atveju, kai IT sistemų vartotojai bus tinkamai informuoti apie riziką bei saugumo priemones, kuriomis reikia naudotis norint apsisaugoti nuo kibernetinių atakų. IT paslaugų tiekėjams ir operatoriams gali tekti prisiimti didesnę atsakomybę, nes jie turės teikti ne tik savo produktus, bet kartu tiekti vartotojams atitinkamus saugumo produktus.

3. **IT saugumo stiprinimas viešajame sektoriuje**

Bus sustiprinta viešojo sektoriaus IT sistemų apsauga. Valstybinės valdžios institucijos privalo būti kaip pavyzdys ir demonstruoti duomenų saugumo svarbą. Tam yra svarbus operatyvinis bendradarbiavimas su CERT (kompiuterinių incidentų tyrimų tarnyba; angl. *computer emergency response teams*).

4. **Nacionalinis Kibernetinio Reagavimo Centras**

Siekiant užtikrinti operatyvinį bendravimą tarp visų valstybinių institucijų ir pagerinti reagavimą į kibernetinius incidentus bus įsteigtas Nacionalinis kibernetinio reagavimo centras. Jis bus atsakingas Federaliniui informacijos saugumo centrui ir tiesiogiai bendradarbiaus su Federaline civilinės apsaugos ir nelaimių tarnyba. Įstatymų numatyta tvarka, Federalinės kriminalinės policijos biuras, Federalinė policija, Muitinės kriminologinė tarnyba, Federalinė žvalgybos taryba, Kariuomenė ir kritinių infrastruktūrų tinklų operatoriai dalyvauja Nacionalinio kibernetinio reagavimo centro programoje ir vykdo pavestas užduotis.

Greitas ir saugus informacijos dalijimasis tarp minėtų institucijų apie IT produktų silpnybes ir pažeidžiamumą leistų Nacionaliniam kibernetinio reagavimo centrui analizuoti kibernetinius incidentus ir suteikti institucijoms informaciją ir veiksmų rekomendacijas kaip apsisaugoti. Taip pat, labai svarbi ir privataus sektoriaus apsauga nuo kibernetinių nusikaltimų.

5. **Nacionalinė Kibernetinio Saugumo Taryba**

Nacionalinė kibernetinio saugumo taryba nustatys ir pašalins priežastis, dėl kurių gali kilti kibernetinės krizės. Tai bus puiki prevencinė priemonė. Dėl šios priežasties yra svarbu palaikyti Federacinės Vyriausybės bendradarbiavimą su viešuoju ir privačiuoju sektoriumi. Nacionalinė kibernetinio saugumo taryba bendradarbiaus su užsienio reikalų, vidaus reikalų, gynybos, ekonomikos ir technologijų, teisingumo finansų ir švietimo ministerijomis. Ypatingais atvejais bus įtrauktos kitos ministerijos bei atstovai iš akademinės aplinkos. Taip pat, bendradarbiaujant dalyvaus verslo atstovai. Pagrindinis Nacionalinės kibernetinio saugumo tarybos siekis yra koordinuoti prevencines priemones ir metodus viešajame ir privačiame sektoriuose.

6. **Veiksminga nusikalstamumo kontrolė kibernetinė erdvėje**

Privalo būti sustiprinta privačiojo sektoriaus apsauga siekiant apsisaugoti nuo šnipinėjimo ir sabotažo. Siekiant pagerinti keitimąsi praktinėmis žiniomis šioje srityje yra ketinama steigti bendras institucijas bendradarbiaujant su kompetentingomis teisėsaugos institucijomis, kuriuos būtų kaip patarėjos.

7. **Efektyvūs suderinti veiksmai siekiant užtikrinti kibernetinį saugumą Europoje ir visame pasaulyje**

Pasaulinis kibernetinės erdvės saugumas gali būti užtikrintas tik pasitelkiant suderintas priemones veikiant nacionaliniu ir tarptautiniu lygiu. Bus siekiama suformuoti išorinę Vokietijos kibernetinę politiką taip, kad Vokietijos idėjos ir interesai susiję su kibernetiniu saugumu būtų

koordinuojami tokių organizacijų kaip Jungtinės Tautos, ESBO, Europos Tarybos, EBPO ir NATO. Vokietija pasisako už vienodus saugumo standartus NATO aljanso šalyse.

8. Patikimų informacinių technologijų naudojimas

Patikimų IT sistemų ir jų sudedamųjų dalių naudojimas turi būti užtikrintas. Siekiant šio tikslo bus aktyviai plėtojami moksliniai tyrimai IT saugumo srityje. Vokietijos tikslas yra naudoti saugumo priemones, kurios atitinka tarptautinius sertifikavimo standartus.

9. Federalinės valdžios personalo plėtra

Atsižvelgiant į kibernetinio saugumo svarbą būtina užtikrinti reikiamą saugumo specialistų skaičių valdžios institucijose.

10. Priemonės, skirtos reaguoti į kibernetines atakas

Jei valstybė nori būti pasirengusi kibernetinėms atakoms turi būti sukurtos priemonių rinkinys, bendradarbiaujant su kompetentingomis valstybės institucijomis. Jei reikia, turi būti patikrinti, ar papildyti įstatymų įgaliojimai.

Darnus strategijos įgyvendinimas

Vadovaudamasi strateginiais tikslais ir priemonėmis Vokietijos Federacinė Vyriausybė sieks užtikrinti kibernetinį saugumą šalyje. Daug kas priklausys nuo to, ar pavyks tarptautiniu mastu imtis atsargumo priemonių siekiant apsaugoti kibernetinę erdvę. Informacinių technologijų naudojimas techniniais ir socialiniais aspektais turi būti įvertintas, nes informacinės technologijos su savo nauda gali sukelti ir naujų pavojų, tokių kaip kibernetiniai incidentai, nusikaltimai elektroninėje erdvėje. Būtent dėl šios priežasties Federalinė Vyriausybė reguliariai prižiūrės ir tikrins, ar iškelti strateginiai tikslai bus pasiekti vadovaujantis Nacionalinio kibernetinio saugumo tarybos sprendimais bei taikys strategijas ir priemones kaip tuos tikslus būtų tikslingiau įgyvendinti.

1.6 Austrijos kibernetinio saugumo strategija

Austrijoje maždaug trys ketvirtadaliai gyventojų reguliariai naudojasi internetu, o pusė jų tai daro kasdien. Austrijos kibernetinio saugumo strategijos (*Austrian Cyber Security Strategy,* 2013) pagrindinis *prioritetas yra užtikrinti elektroninės erdvės saugumą ir patikimumą tiek nacionaliniu, tiek ir tarptautiniu lygiu.*

Austrijos kibernetinio saugumo strategijoje (ACSS) yra pateikiama išsami koncepcija kaip apsaugoti elektroninę erdvę bei asmenis, kurie veikia virtualioje erdvėje užtikrinant ir garantuojant žmogaus teises.

Austrijos Kibernetinio Saugumo Strategija buvo sukurta remiantis Saugumo Strategija bei vadovaujantis Austrijos Programa Kritinėms Infrastruktūroms Apsaugoti principais.

Remiantis Austrijos Kibernetinio Saugumo Strategija, saugumo politika neturi apsiriboti tik nacionalinėmis valstybių sienomis – apsauga privalo būti užtikrinta tarptautiniu lygmeniu. Tai reikalauja glaudaus tarptautinio bendradarbiavimo.

Principai

Kibernetinio saugumo politika turi apimti daugelį gyvenimo sričių. Ji turi būti modeliuojama remiantis išsamiu ir integruotu požiūriu. Svarbus aktyvus dalyvavimas ir solidarumas. Išsami kibernetinio saugumo politika reiškia tai, kad civiliai ir kariniai aspektai yra glaudžiai tarpusavyje susiję. Kibernetinis saugumas apima tradicines saugumo ir politikos institucijas.

Kibernetinio saugumo politika turi būti integruota visuotinai. Ji apima tokias sritis kaip: politinis strateginis valdymas, švietimas ir mokymas, rizikos vertinimas, prevencija ir parengtis.

Saugumo politika turi būti grindžiama bendradarbiavimu tarptautiniu ir nacionaliniu lygmeniu. Saugumo politikos esmė yra užkirsti kelią grėsmės elektroninėje erdvėje, arba sušvelninti jų poveikį.

Kibernetinio saugumo politika yra paremta solidarumu. Atsižvelgiant į tai, kad elektroninė erdvė yra visuotinė, tai negali būti atskirai tik Austrijos elektroninės erdvės saugumo problema. Tai yra visų Europos Sąjungos narių ir visos likusios tautos problema. Politika turi būti grindžiama solidarumo principu.

Pagrindiniai principai, užtikrinantys Austrijos skaitmeninės apsaugos sritį yra: konfidencialumas, vientisumas, autentiškumas, prieinamumas, privatumo ir duomenų apsauga.

Pagrindiniai principai taikomi kibernetinio saugumo srityje

1. **Teisės aktų laikymasis**. Kibernetinio saugumo valdymas turi atitikti aukštus Austrijos teisinius administravimo standartus, nepažeisti žmogaus teisių, taip pat garantuoti privatumo ir duomenų apsaugą bei saviraiškos laisvę ir teisę į informacijos prieinamumą.
2. **Subsidiarumas**. Kibernetinis saugumas teisiškai yra turtas, todėl valstybė įsipareigoja jį ginti. Tačiau valstybė negali prisiimti visos atsakomybės ginant kibernetinę erdvę. Informacijos ir ryšių operatoriai, yra tiesiogiai atsakingi už savo sistemų apsaugą.
3. **Savireguliacija.** Kibernetinis atsparumas turėtų būti pasiektas pačių suinteresuotųjų šalių pastangomis. Tai turėtų būti paremta pripažinto standartizavimo, sertifikavimo pagrindu. Tokiomis priemonėmis būtų sudaryta reguliavimo sistema, kuri padėtų užtikrinti įmonių ir privačių asmenų saugumą.
4. **Proporcingumas**. Priemonės, skirtos saugumo lygiui didinti ir joms skirti kaštai turi būti proporcingi atitinkamos rizikos ir jos grėsmės ribojimo galimybėms.

Remiantis šiais principais yra kuriama nuosekli saugumo politika tarptautiniu ir nacionaliniu lygiu, kuri padeda:

- plėtoti saugią elektroninę erdvę atsižvelgiant į piliečių, akademinės visuomenės ir valstybės interesus;
- išvengti grėsmių elektroninėje erdvėje bei atlieka jų prevenciją;

- vertinti kaip turtą “kibernetinį saugumą” kaip turtą ir apsaugoti jį nuo grėsmių, o taip pat, joms kilus, su jomis susidoroti.

Strateginiai tikslai

Dinamiška virtuali elektroninė erdvė palengvina socialinę gerovę bei teikia ekonominę naudą iš e-komercijos ir e-valdžios sistemų. Ji palengvina informacijos keitimosi funkcijas bei tampa politinio ir socialinio bendradarbiavimo priemone.

Atsižvelgdama į savo kibernetinio saugumo strategiją, Austrijos pagrindiniai strateginiai tikslai yra šie:

1. Duomenų prieinamumas, patikimumas ir konfidencialumas gali būti užtikrintas tik saugioje ir patikimoje elektroninėje erdvėje. Virtuali erdvė privalo būti atspari rizikos veiksniams, atakoms, turi prisitaikyti prie pakitusios aplinkos;
2. Nacionaliniu požiūriu, kompetentingos Austrijos federalinės ministerijos užtikrins, kad informacinių ir ryšių technologijų ICT (angl. Information and communications technology) infrastruktūros būtų saugios ir atsparios grėsmėms. Užtikrintas viešojo ir privataus sektoriaus bendradarbiavimas;
3. “Kibernetinis saugumas”, kaip turtas, yra saugomas Austrijos valdžios institucijų;
4. Teikiant informaciją apie kibernetinio saugumo svarbą, Austrijoje yra formuojama “kibernetinio saugumo kultūra”;
5. Įgyvendinusi minėtus tikslus Austrija tampa patraukli verslo vieta investuotojams;
6. Austrija atlieka svarbų vaidmenį vykdant tarptautinį bendradarbiavimą Europos ir pasaulio mastu, ypač keičiantis informacija bei patirtimi formuojant tarptautines strategijas;
7. Stiprinama ir plėtojama Austrijos e-valdžios apsauga;
8. Bus apsaugotas visų Austrijos įmonių naudojamų programų vientisumas, o taip pat, užtikrinama asmens duomenų privatumo apsauga įmonių klientams. Glaudus ir sistemingas bendradarbiavimas tarp įmonių vaidina lemiamą vaidmenį šiame procese;
9. Austrijos gyventojai privalo žinoti savo asmeninę atsakomybę elektroninėje erdvėje. Visi piliečiai privalo naudotis elektronine erdve deramai, būti atsakingi už savo veiklą naudojantis internetu.

Veiksmų sritys ir priemonės

Veiksmų sritis - struktūros ir procesai

Pagrindinis tikslas - yra keletas organizacijų, kurios specializuojasi kibernetinio saugumo srityje, pavyzdžiui – CERT, kuris dabar atlieka svarbų vaidmenį krizių valdymo srityje. Yra ir daugybė institucijų ir suinteresuotųjų šalių, kurių darbas yra užtikrinti kibernetinės erdvės saugumą. Tačiau iki šiol svarbiausios kibernetinio saugumo procedūros nebuvo apibrėžtos oficialiai. Todėl yra

būtina tiksliai apibrėžti procesus, kurie užtikrins visuotinį koordinavimą strateginiu lygiu tarp viešojo ir privataus sektoriaus.

Priemonės:

1. **Kibernetinio saugumo iniciatyvinės grupės steigimas**

2012 liepos 11 d. Ministrų taryba nusprendė įsteigti *Kibernetinio Saugumo Iniciatyvinę Grupę*. Ji yra atsakinga už priemonių, susijusių su kibernetiniu saugumu koordinavimu politiniu-strateginiu lygiu, stebėsenos ir rėmimo procesus įgyvendinant Austrijos kibernetinio saugumo strategiją ACSS (angl. Austrian Cyber Security Strategy). *Kibernetinio Saugumo Iniciatyvinė Grupė* rengia ataskaitas ir pataria federalinei vyriausybei visais klausimais, susijusiais su kibernetiniu saugumu. *Kibernetinio Saugumo Iniciatyvinė Grupė* yra sudaryta iš ryšių palaikymo pareigūnų bei kibernetinio saugumo ekspertų priklausančių Nacionalinei saugumo tarybai. Taip pat šiai grupei priklauso Vyriausiasis Austrijos Federacinės Respublikos informacijos pareigūnas ir kiti atstovai iš ministerijų.

2. **Veiklos koordinavimo struktūros sukūrimas**

Remiantis esamomis struktūromis bus sukurta nauja struktūra, kuri pasitarnaus kaip platforma, naudojama svarstant priemones, kurių reiktų imtis kibernetinio incidento atveju. Taip pat šios platformos pagalba bus atliekama apžvalga elektroninėje erdvėje, renkama, perduodama ir vertinama informacija, atliekamos prevencinės ir reagavimo procedūros. Bus analizuojama interneto keliama grėsmė. *Ši platforma bus naudojama kaip pagrindinis organas, vykdantis kibernetinių krizių valdymą.*

Struktūra bus sudaryta iš tokių valstybinio lygmens organizacijų kaip: GovCERT (nacionalinio ryšių reguliavimo tarnybos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys), Karinė kibernetinio saugumo kritinės parengties komanda MilCERT (Military Cyber Emergency Readiness Team) ir Elektroninių nusikaltimų kompetencijos centras C4 (angl. Cyber Crime Competence Center). *Aiški struktūra ir funkcijos*.

3. **Kibernetinių krizių valdymo centro steigimas**

Krizių valdymo planai bus rengiami ir nuolat atnaujinami remiantis rizikos analize. Kiekvienam atskiram sektoriui bus pritaikyta atitinkama kibernetinių grėsmių rizikos analizė. Ši analizė bus atliekama bendradarbiaujant su ypatingos svarbos infrastruktūros objektų operatoriais.

4. **Esamų kibernetinių saugumo struktūrų stiprinimas**

Siekiama sustiprinti GovCERT, MilCERT ir C4 vaidmenį. Tai bus atliekama detaliai nustatant atsakomybes ir įgaliojimus. Bus apibrėžtas vaidmuo kibernetinės krizės atveju, taip pat nustatyta sąveika su Veiklos Koordinavimo Struktūra.

Veiksmų sritis – valdymas

Pagrindinis tikslas – apibrėžti valstybinių ir nevalstybinių subjektų vaidmenis, atsakomybes ir įgaliojimus elektroninėje erdvėje ir sukurti tinkamas sąlygas bendradarbiavimui tarp šių dalyvių.

Priemonės:

5. **Sukurti modernią reguliavimo sistemą**

Išanalizavus Kibernetinio saugumo iniciatyvinės grupės parengtą ataskaitą ir nustačius poreikį, sukurti reguliavimo priemones (elgesio kodeksą), kuris garantuotų kibernetinį saugumą Austrijoje ir būtų patvirtintas federalinės vyriausybės. Ši ataskaita apims tokias sritis kaip: reikiamų organizacinių struktūrų kūrimą, užduotis ir įgaliojimus valdžios institucijoms, keitimasis informacija tarp institucijų ir privačių asmenų, ataskaitų rengimo pareigas ir kt.

6. **Minimalių standartų nustatymas**

Atsižvelgiant į visas suinteresuotąsias šalis nustatyti minimalius apsaugos standartus, kurie užtikrintų veiksmingą prevenciją. Šie reikalavimai bus taikomi visose ICT paslaugų srityse.

7. **Metinės ataskaitos apie kibernetinį saugumą rengimas**

Kibernetinio saugumo iniciatyvinė grupė parengs metinę ataskaitą „Kibernetinis saugumas Austrijoje“.

Veiksmų sritis – bendradarbiavimas tarp valdžios institucijų, verslo subjektų ir visuomenės

Pagrindinis tikslas – daugelis kasdienių sričių ir užduočių viešojo administravimo sektoriuje, ekonomikos sektoriuje ir tarp paprastų piliečių yra paremtas informacinėmis ir ryšių technologijomis. Atsakomybė už savo atliktus veiksmus, naudojantis skaitmeninėmis technologijomis, turėtų tekti kiekvienam iš išvardintų objektų. Tačiau tai galima būtų užtikrinti tik jei būtų nuolat keičiamasi informacija, kuri leistų sužinoti, ar naudojimasis informacinėmis ir ryšių priemonėmis yra saugus. Tokiu būdu būtų atrastos spragos bei būtų aišku, kuriame lygmenyje jos saugumas buvo pažeistas.

Priemonės:

8. **Kibernetinio Saugumo Platformos sukūrimas**

Austrijos Kibernetinio Saugumo Platforma bus įsteigta kai viešojo ir privataus sektorių partnerystė, kurios tikslas palengvinti bendravimą tarp visų viešojo administravimo subjektų, verslo subjektų ir akademinės bendruomenės. Kibernetinio Saugumo Platformai pataria ir ją palaiko Kibernetinio Saugumo Iniciatyvinė Grupė.

Taip pat, šios platformos dėka galėtų bendradarbiauti ypatingos svarbos infrastruktūros objektai ir ryšių operatoriai. Platforma padės informuotumo didinimo, mokymo, o taip pat mokslinių tyrimų plėtros procesui užtikrinti.

9. **Stiprinti paramą mažoms ir vidutinėms įmonėms**

Bus stiprinama mažų ir vidutinių įmonių apsauga kibernetinio saugumo srityje, skatinamas informuotumas ir pasiruošimas kibernetiniams incidentams. Turi būti viešai skelbiama informacija internete, portale *ICT Security* (liet. Informacijos ir ryšių saugumas) apie galimą pavojų mažoms ir vidutinėms įmonėms. Kartu su Vyriausybinių įstaigų parama būtų paskelbti rizikos valdymo planai konkretiems sektoriams. Šie planai bus rengiami periodiškai. Konkretiems mažų ir vidutinių įmonių sektoriams būtų leidžiama dalyvauti kibernetiniuose mokymuose (angl. *cyber exercises*).

10. **Kibernetinio saugumo komunikacijos strategijos ruošimas**

Siekiant optimizuoti komunikaciją tarp suinteresuotųjų šalių viešojo administravimo sektoriuje, ekonomikos sektoriuje, mokslo aplinkoje ir visuomenėje Kibernetinio Saugumo Iniciatyvinė Grupė parengtų komunikacijos strategiją, kurios dalyviai būtų visos išvardintos suinteresuotosios grupės.

Veiksmų sritis – kritinių infrastruktūrų apsauga

Pagrindinis tikslas – užtikrinti kritinių infrastruktūrų apsaugą, nes beveik visa šių dienų infrastruktūra naudoja IT sistemas savo veikloje. Tikimąsi, kad bus užtikrintas sklandus, patikimas ir nenutrūkstantis IT sistemų veikimas, susijęs su kritinės infrastruktūros veikla. Pagrindinis prioritetas yra užtikrinti šių sistemų atsparumą kibernetinėms grėsmėms.

Vadovaujantis Austrijos programa dėl kritinių infrastruktūrų apsaugos (vok. *Programm zum Schutz kritischer Infrastrukturen/ APCIP*), įmonės bus skatinamos įgyvendinti visapusišką saugumo architektūrą. Austrijos kibernetinio saugumo strategija yra papildoma *APCIP* priemonėmis kibernetinio saugumo srityje.

Priemonės:

11. **Kritinės svarbos infrastruktūrų atsparumo gerinimas**

Kritinės svarbos infrastruktūrų objektų ryšio operatoriai turėtų būti įtraukti į visus nacionalinių procesų krizių valdymus. Šios strategiškai svarbios įmonės turi vykdyti visapusišką rizikos valdymą atsižvelgiant į pagrindines grėsmes. Taip pat, kritinių infrastruktūrų objektų ir ryšio operatorių partnerystė turi būti nustatyta remiantis saugumo standartais.

Kritinės svarbos infrastruktūrų objektų ryšio operatoriai būtų įpareigoti pranešti apie sunkius kibernetinius nusikaltimus.

Veiksmų sritis – sąmoningumo didinimas ir mokymas

Pagrindinis tikslas – suteikti kuo daugiau žinių ir supratimo apie kibernetinio saugumo svarbą. Būtina didinti žinias ir skatinti sąmoningą elgesį kibernetinėje.

Priemonės:

12. **Kibernetinio saugumo kultūros formavimas**

Turi būti plėtojamos sąmoningumo didinimo iniciatyvos. Svarbu pažvelgti į kibernetinį saugumą iš skirtingų perspektyvų, išryškinti svarbius pavojus, siekiant atkreipti dėmesį į galimą poveikį ir žalą.

Bus įsteigtas interneto portalas *ICT Security,* kuris bus kaip komunikacijos ir informuotumo didinimo priemonė.

13. **Diegti kibernetinio saugumo supratimą žiniasklaidoje ir švietimo įstaigose**

Svarbu sustipinti kibernetini saugumo svarbą mokyklų programose. Informacijos ir komunikacijos priemonių naudojimo saugumo svarba turi būti akcentuojama visose mokyklose.

1.6.1.1 Veiksmų sritis – moksliniai tyrimai ir plėtra

Pagrindinis tikslas – siekiant užtikrinti kibernetinį saugumą būtina užtikrinti atitinkamas technines žinias, kurios būti grindžiamos valstybės mokslinių tyrimų plėtros rezultatais. Būtina stiprinti taikomųjų mokslų programas, kuriose akcentuojamas kibernetinis saugumas. Svarbus aktyvus dalyvavimas ES saugumo mokslinėse programose.

Priemonės:

14. **Austrijos mokslinių tyrimų stiprinimas susijusių su kibernetiniu saugumu**

Atsižvelgiant į nacionalinių ir ES mokslinių tyrimų programų saugumo srityje svarbą reikia užtikrinti, kad kibernetinio saugumo užtikrinimas Austrijoje būtų mokslinių tyrimų prioritetu.

Veiksmų sritis – tarptautinis bendradarbiavimas

Pagrindinis tikslas – tarptautinis bendradarbiavimas yra vienas iš svarbiausių Austrijos kibernetinio saugumo strategijos tikslų. Saugumas turi būti užtikrintas derinant nacionalinio ir tarptautinio lygio aspektus. Austrija privalo užsiimti aktyvia kibernetinio saugumo politika ir bendradarbiauti su tokiomis organizacijomis kaip ES, JT, ESBO, Europos Taryba, NATO.

Priemonės:

15. **Efektyvus bendradarbiavimas siekiant kibernetinio saugumo Europoje ir pasaulyje**

- Austrija prisidėjo prie ES kibernetinio saugumo strategijos kūrimo ir įgyvendinamo. Kompetentingos ministerijos imsis reikiamų veiksmų priemonių, kad Austrijoje būtų visapusiškai įgyvendinta Konvencija dėl elektroninių nusikaltimų (Konvencija dėl elektroninių nusikaltimų, Budapeštas, 2001);
- Austrija pasisako už laisvą internetą tarptautiniu lygiu. Žmogaus teisės turi būti užtikrinamos elektrinėje erdvėje, o ypatingai laisvė į informaciją;
- Austrija aktyviai tęsia bendradarbiavimą su NATO;
- Austrija aktyviai dalyvauja įgyvendinant tarptautines kibernetines pratybas.

Strategijos vykdymas

Kai federalinė vyriausybė patvirtina Austrijos kibernetinio saugumo strategiją, Iniciatyvinė grupė per tris mėnesius, plėtoja strategijos įgyvendinimo planą pasitelkdama priemones,

nustatytas ACSS. Už strategijos įgyvendinimą ir priemonių pritaikymą yra atsakingos kompetentingos institucijos. Remiantis ACSS, ministerijos plėtos strateginius pogrupius, atsižvelgiant į savo veiklos sritį. Ministerijų atstovai, priklausantys *Kibernetinio Saugumo Iniciatyvinei Grupei* turės kas dvejus metus pateikti veiklos ataskaitą federalinei vyriausybei. Veiklos ataskaita bus vertinama ir atsižvelgus į vertinimą, Kibernetinio saugumo strategija bus nuolat plėtojama.

1.7 Vokietijos ir Austrijos strategijų apibendrinantys lyginamieji aspektai

Remiantis atlikta Austrijos ir Vokietijos kibernetinio saugumo strategijų analize matyti, kad strateginiai tikslai ir principai abiejose strategijose turi panašumų. Galima išskirti šiuos kibernetinio saugumo reguliavimo panašumus:

1. Austrijos ir Vokietijos strateginiai tikslai iš dalies sutampa, išskirtas ypatingos svarbos informacinės infrastruktūros objektų apsaugos svarbumas; institucijos, atsakingos už operatyvinį bendravimą tarp visų valstybinių institucijų steigimas; bendradarbiavimas su tarptautinėmis organizacijomis.
2. Tiek Austrijos, tiek ir Vokietijos strategija numato, kad būtina reguliuoti kibernetinio saugumo procesus ne tik nacionaliniu, bet ir tarptautiniu lygiu. Remiantis Austrijos Kibernetinio Saugumo Strategija, saugumo politika neturi apsiriboti tik nacionalinėmis valstybių sienomis – apsauga privalo būti užtikrinta tarptautiniu lygmeniu. Tai reikalauja glaudaus tarptautinio bendradarbiavimo. Pagrindinis Vokietijos kibernetinio saugumo strategijos siekis yra užtikrinti darnią tarptautinę kibernetinę erdvę.
3. Pagrindiniai uždaviniai tiek Austrijos, tiek ir Vokietijos skaitmeninės apsaugos srityje yra užtikrinti elektroninės informacijos konfidencialumą, vientisumą, autentiškumą, prieinamumą.
4. Abiejose kibernetinio saugumo strategijos akcentuojamas dėmesys į tai, kad norint pasiekti maksimalių rezultatų privalomas viešojo ir privačiojo sektoriaus bendradarbiavimas.
5. Abiejose strategijose išskirta glaudaus bendradarbiavimo svarba su CERT (kompiuterinių incidentų tyrimų tarnyba; angl. *Computer emergency response teams*), kuri atlieka svarbų vaidmenį krizių valdymo srityje.
6. Tiek Austrijos, tiek Vokietijos kibernetinio saugumo strategijose sutampa strateginis tikslas – įsteigti instituciją (Austrija - *Kibernetinio Saugumo Iniciatyvinė Grupė;* Vokietija - *Nacionalinis kibernetinio reagavimo centras*), kuri būtų atsakinga už priemonių, susijusių su kibernetiniu saugumu koordinavimu. Ši institucija analizuoti kibernetinius incidentus ir suteikti atitinkamoms institucijoms informaciją ir veiksmų rekomendacijas kaip apsisaugoti nuo kibernetinių krizių. Lietuvos atveju, tokia

atitinkanti institucija būtų *Kibernetinio saugumo centras*, kuris šalyje yra atsakingas už su valstybės informaciniais ištekliais ir ypatingos svarbos informacine infrastruktūra susijusių institucijų kibernetinio saugumo valdymą.

Pagrindiniai skirtumai tarp šių strategijų yra tokie, kad Austrijos strategija, apibūdindama strateginius tikslus aiškiai išskiria veiklos sritis bei tikslingai įvardina veiksmus ir priemones, kurių imsis ir kurios bus naudojamos norint įgyvendinti strateginius tikslus.

Vokietijos strategijoje, skirtingai nei Austrijos, įvardintos tik strateginės kryptys, kuriose turėtų būti atlikti veiksmai, tačiau neįvardinti konkretūs veiksmai ir priemonės, kurių turi būti imamasi.

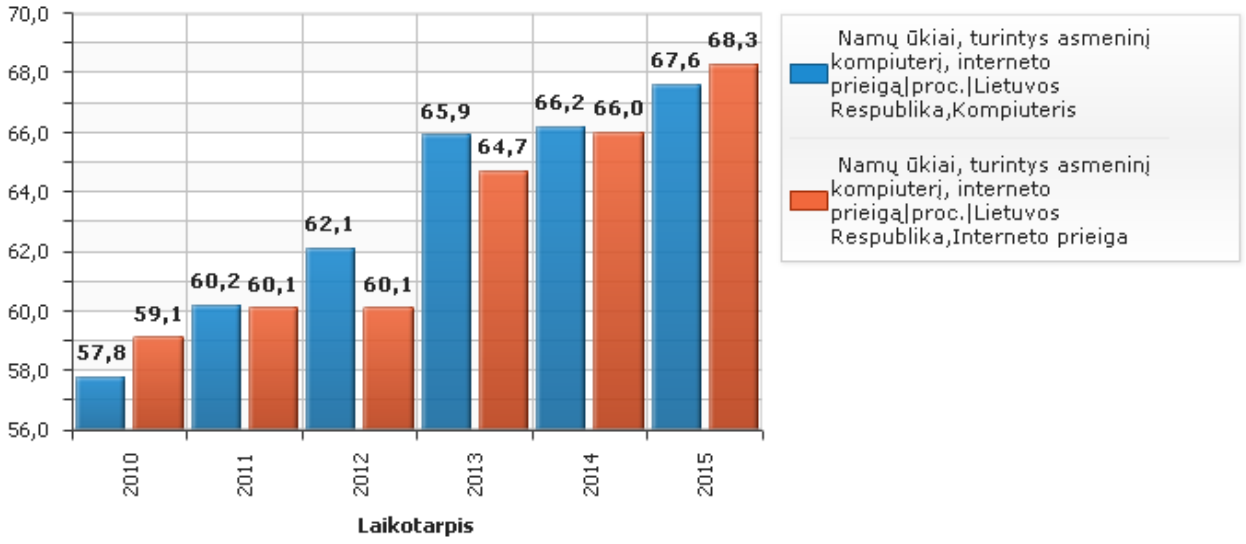
Skirtingai nei Vokietijos, Austrijos kibernetinio saugumo strategijoje pabrėžiama, kad teikiant vartotojams informaciją apie kibernetinio saugumo svarbą, yra formuojama "kibernetinio saugumo kultūra". Svarbu sustipinti kibernetinio saugumo svarbą mokyklų programose. Informacijos ir ryšių priemonių naudojimo saugumo svarba turi būti akcentuojama visose mokyklose.

Lietuvos kibernetinio saugumo plėtros 2011–2019 metais programoje bei Kibernetinio saugumo įstatyme vartotojų informavimas akcentuojamas, kaip vienas iš tikslų, kuriam pasiekti yra būtinas visuomenės švietimas.

Tačiau būtina atkreipti dėmesį į tai, kad kibernetinio saugumo strategija yra valstybei nacionaliniu saugumo mastu svarbus dokumentas, todėl gali būti, kad Vokietija sąmoningai neatskleidžia tam tikrų veiklos krypčių, veiksmų ar detalių, saugodama savo konfidencialumą. Didelį Kibernetinių incidentų skaičių gali lemti ir valstybės geopolitinė situacija ir veiksmai. Politiškai aktyvios ir pasisakančios valstybės gali sulaukti daugiau kibernetinių incidentų nei „ramios" valstybės. Taip pat, kibernetinių incidentų didelį mastą gali lemti puikiai išvystyta interneto infrastruktūra, kuri gali būti kaip jaukas piktavaliams programišiams ir skatinti juos pasinaudoti puikios infrastruktūros teikiamais privalumais atliekant nusikaltimus. Pastebimas santykis tarp šalies ekonominės situacijos ir kibernetinių incidentų skaičiaus. Kuo šalis turtingesnė tuo ji potencialiai patrauklesnė nusikaltėliams.

KIBERNETINIO SAUGUMO SITUACIJA LIETUVOJE

Saugumo užtikrinimas kibernetinėje erdvėje yra svarbus dėl pastaraisiais metais augančio interneto technologijų (IT) naudojimo masto. Augimo tendenciją patvirtina statistiniai duomenys. Tiek individualių vartotojai, tiek įmonių IT plėtra sparčiai augo. Statistikos departamento prie Lietuvos Respublikos Vyriausybės duomenimis, IT naudojimas namų ūkiuose per pastaruosius penkerius metus sparčiai išaugo.

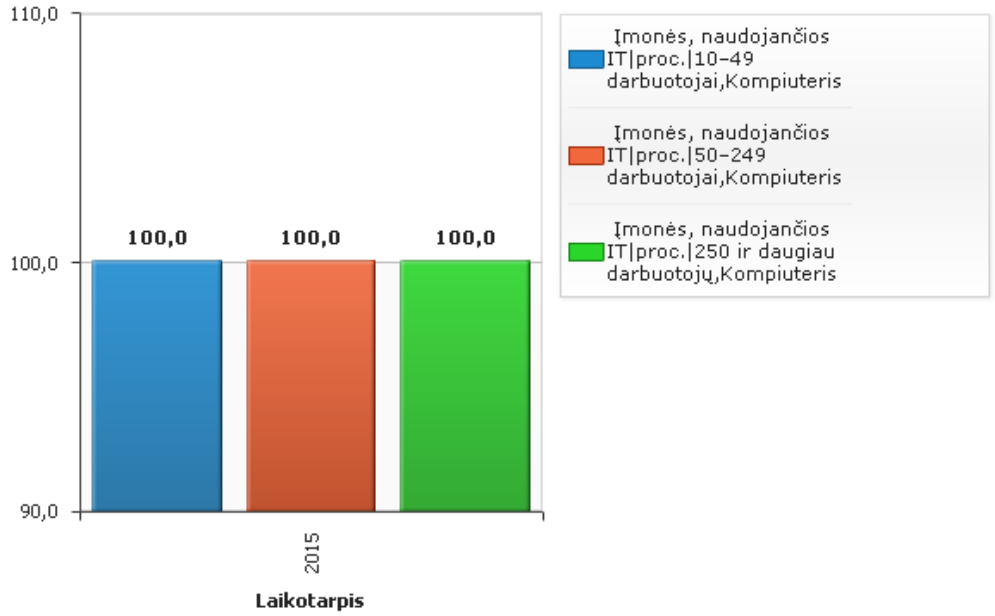


Šaltinis: Lietuvos statistikos departamentas

Pav. 8 **Namų ūkiai turintys kompiuterį ir interneto prieigą**

Nuo 2010 iki 2015 metų namų ūkių, turinčių kompiuterius padidėjo maždaug 10 proc. (nuo 57,8 iki 67,6 proc.). interneto prieigos plėtra taip pat išaugo beveik 10 proc. (nuo 59,1 iki 68,3 proc.). Interneto plėtra sparčiau pradėjo kilti nuo 2012 iki 2015 m. (išaugo 8,2 proc.).

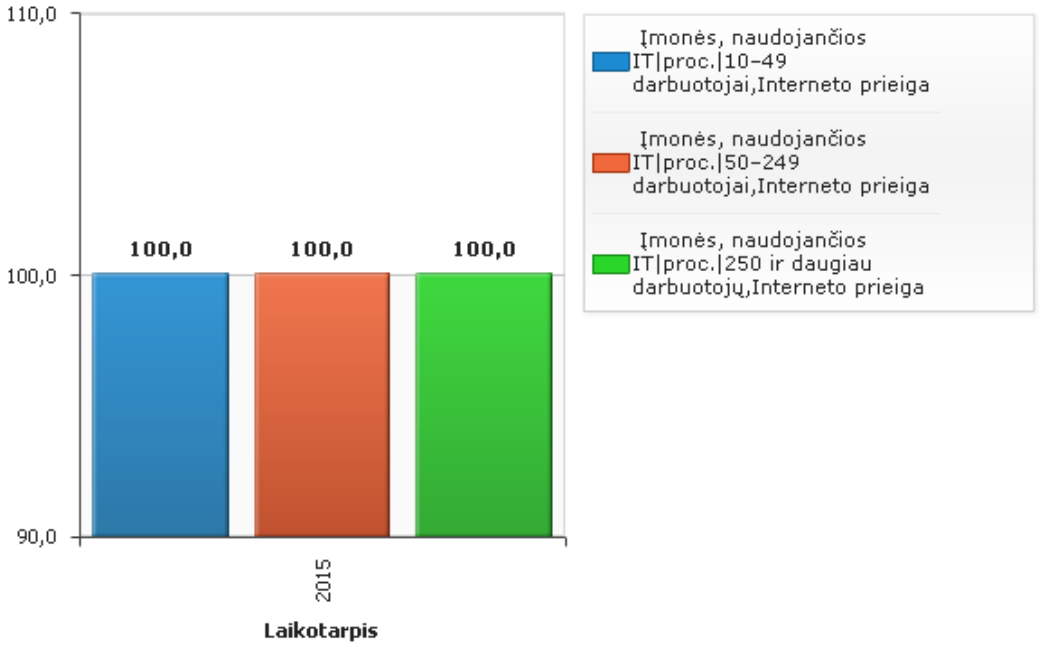
Kalbant apie verslo sektorių – jame taip pat pastebima sparti IT plėtra. 2015 metais net 100 proc. mažų (nuo 10 iki 49 darbuotojų), vidutinių (nuo 49 iki 250 darbuotojų) ir didelių (250 ir daugiau darbuotojų) įmonių, vystant savo veiklą naudojo kompiuterius.



Šaltinis: Lietuvos statistikos departamentas

Pav. 9 **Lietuvos įmonės turinčios naudojančio IT ir turinčios kompiuterius**

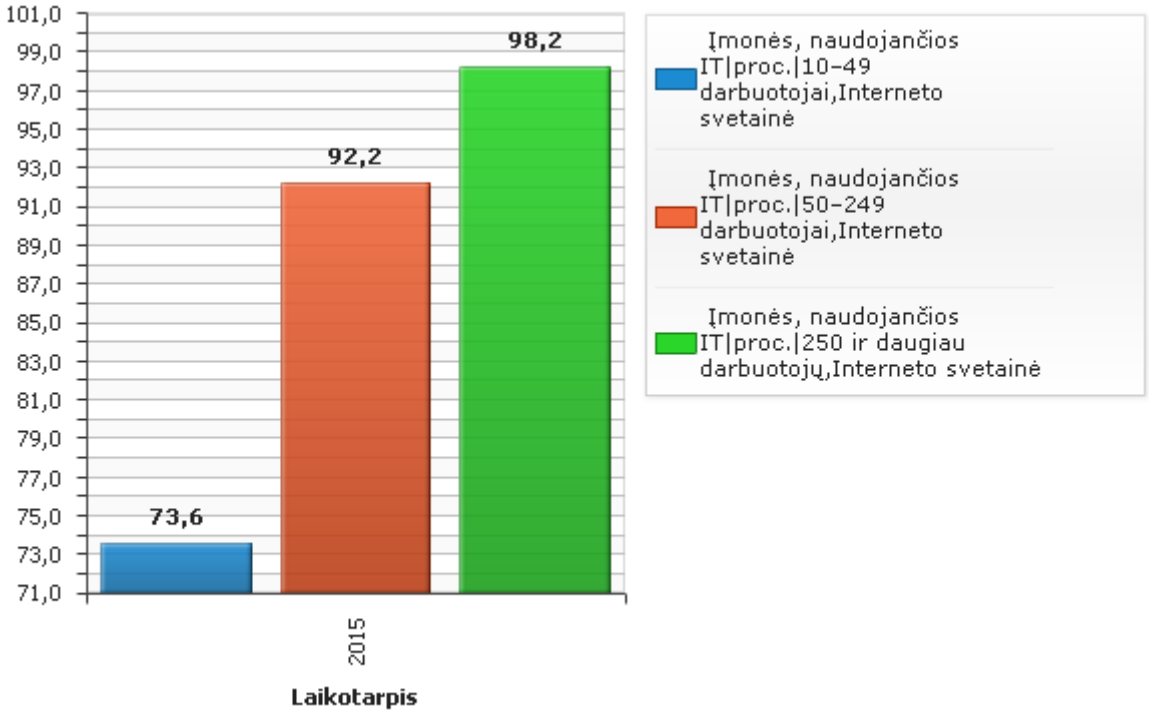
Taip pat 100 proc. mažų, vidutinių ir didelių įmonių, vystant savo veiklą 2015 metais naudojosi interneto prieiga.



Šaltinis: Lietuvos statistikos departamentas

Pav. 10 **Lietuvos įmonės turinčios interneto prieigą**

2015 metų galimybe save reprezentuoti įsigyjant interneto svetainę pasinaudojo 73,6 proc. mažų, 92,2 proc. vidutinių ir net 98,2 proc. didelių įmonių.

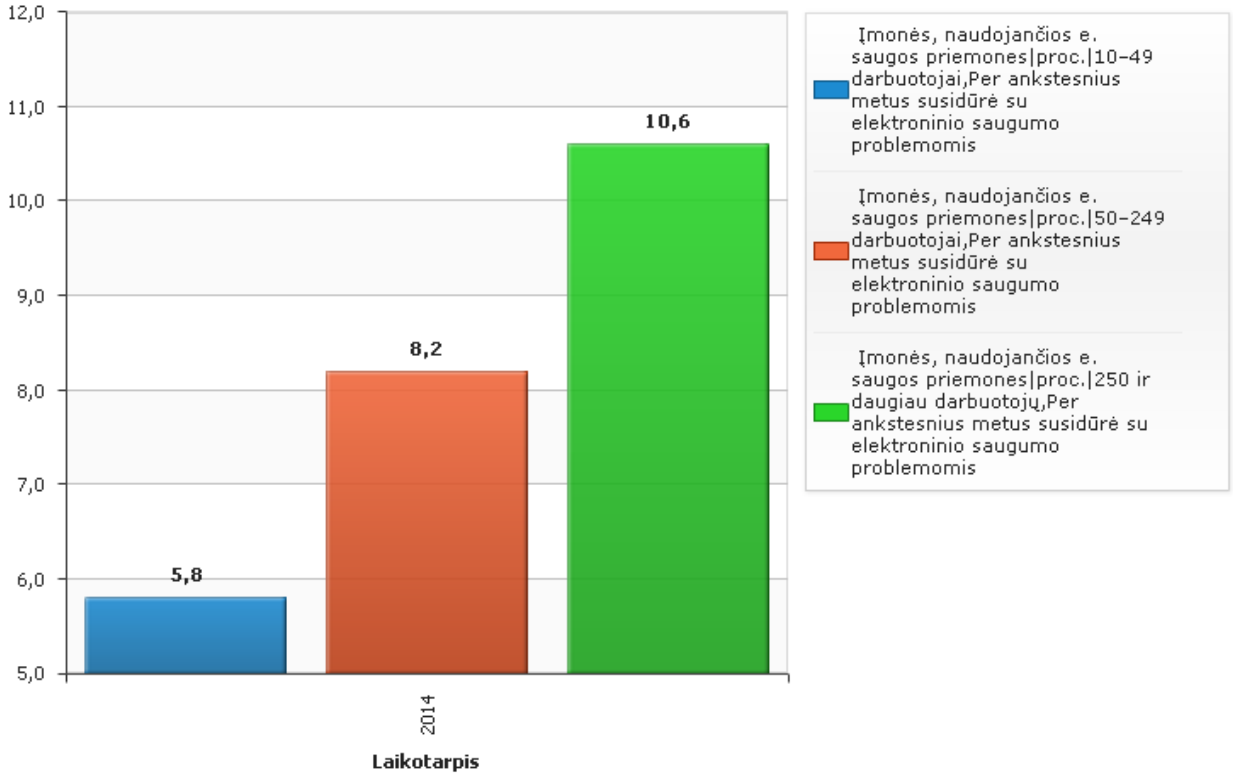


Šaltinis: Lietuvos statistikos departamentas

Pav. 11 **Lietuvos įmonės turinčios interneto svetainę**

Akivaizdu, kad verslo sektorius savo veiklos neįsivaizduoja be galimybės naudotis interneto prieiga. Internetu vyksta visos svarbiausios operacijos – bendravimas su tiekėjais, klientais, vykdomi bankiniai pinigų pavedimai, užsakomos prekės, vykdoma klientų registracija ir daugybė kitų procesų, kurie užtikrina sklandžią verslo plėtra.

Deja, tačiau verslo įmonės susiduriama ir su sunkumais elektroninėje erdvėje. Pastaraisiais metais, su kibernetiniais incidentais susidūrė 5,8 proc. mažų, 8,2 proc. vidutinių ir 10,6 proc. didelių įmonių.



Šaltinis: Lietuvos statistikos departamentas

Pav. 12 **Lietuvos įmonės 2014 metais susidūrusios su elektroninio saugumo problemomis (naudojančios elektroninės saugos priemones)**

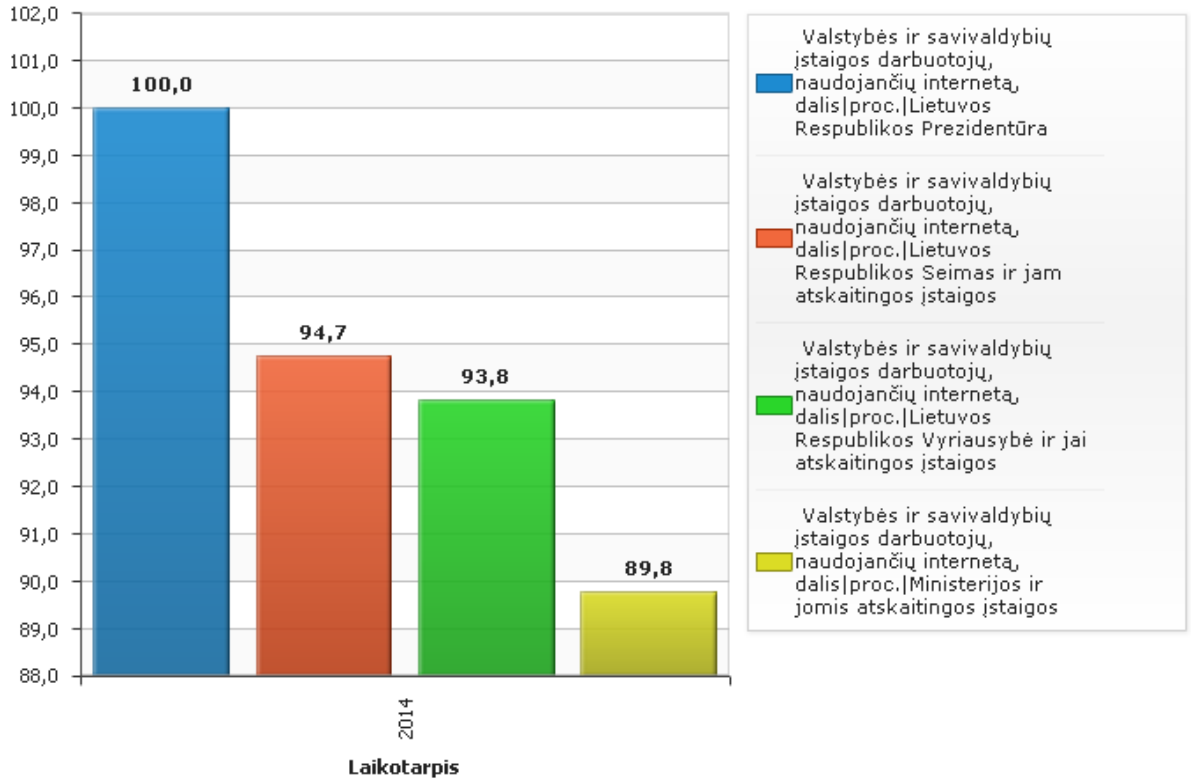
1.8 Kibernetinių nusikaltimų latentiškumas ir žala

Kibernetiniai nusikaltimai yra globalūs, juos gali atlikti nusikaltėlis iš bet kurios pasaulio vietos bet kuriuo laiku. Šios savybės apsunkina nusikaltimų tyrimo procesą, sunkina įrodymų surinkimo tikimybę, todėl nusikaltėlio kaltumą sunku įrodyti teisme. Technologijoms vystantis kibernetinių nusikaltimai tobulėja skaičius auga, jie tobulėja, be abejo, jų žala taip pat sparčiai didėja. Skirtingai nei įprasti nusikaltimai, kibernetiniai nusikaltimai turi stiprią latentiškumo savybę. Oficiali statistika dažnai gali neatspindėti tikrosios nusikaltimų situacijos. Pavyzdžiui, 2010 m. kompanija Google patyrė kibernetinę ataką. Kartu su ja atakas patyrė žymiai daugiau kompanijų, tačiau tai išaiškėjo tik tuomet kai buvo paviešinta WikiLeaks. Tik viena kompanija 2010 m. pripažino, kad prieš ją buvo atlikta kibernetinė ataka tuo metu kaip ir prieš kompaniją Google. Tačiau pastaroji kompanija nepateikė jokių išsamių detalių dėl nusikaltimo padarinių. Taip pat, kai buvo įvykdytas kibernetinis išpuolis prieš pagrindinį JAV banką ir bankas patyrė keleto milijonų JAV dolerių žalą, viešumoje tai buvo slepiama.

Tokį stiprų kibernetinių nusikaltimų latentiškumą lemia keli veiksniai:

1. Kompiuterių naudotojams dažnai trūksta žinių, kad pastebėtų tokius nusikaltimus.

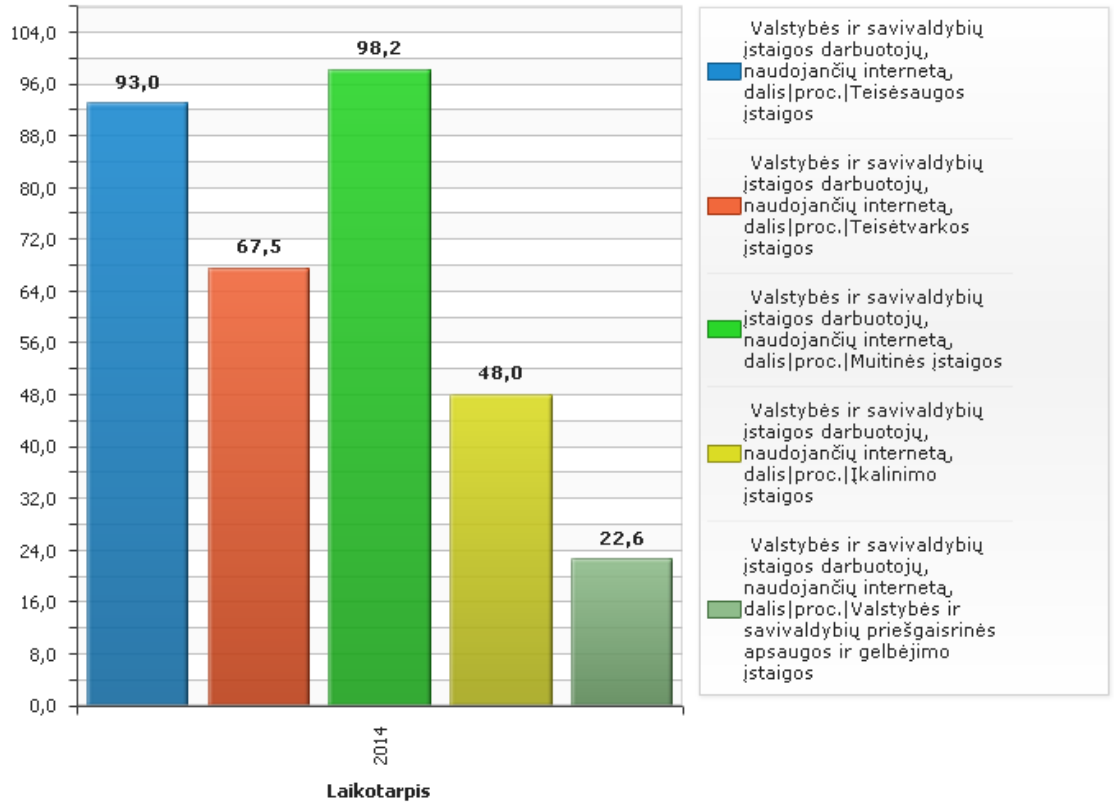
Lietuvoje, didžioji dauguma valstybės ir savivaldybių įstaigų darbuotojų, savo darbuose naudoja internetą. Lietuvos Respublikos Prezidentūroje net 100 proc. darbuotojų, LR Seime ir jam atskaitingose įstaigose 94,7 proc., LR Vyriausybėje ir jai atskaitingose įstaigose 93,8 proc., Ministerijose ir joms atskaitingose įstaigose 89,8 proc. darbuotojų dirbdami naudojasi internetu.



Šaltinis: Lietuvos statistikos departamentas

Pav. 13 **Valstybės ir savivaldybių įstaigų (LR Prezidentūros, LR Seimo ir jam atskaitingų įstaigų, LR Vyriausybės ir jai atskaitingų įstaigų, Ministerijų ir joms atskaitingų įstaigų) darbuotojų, naudojančių internetą dalis**

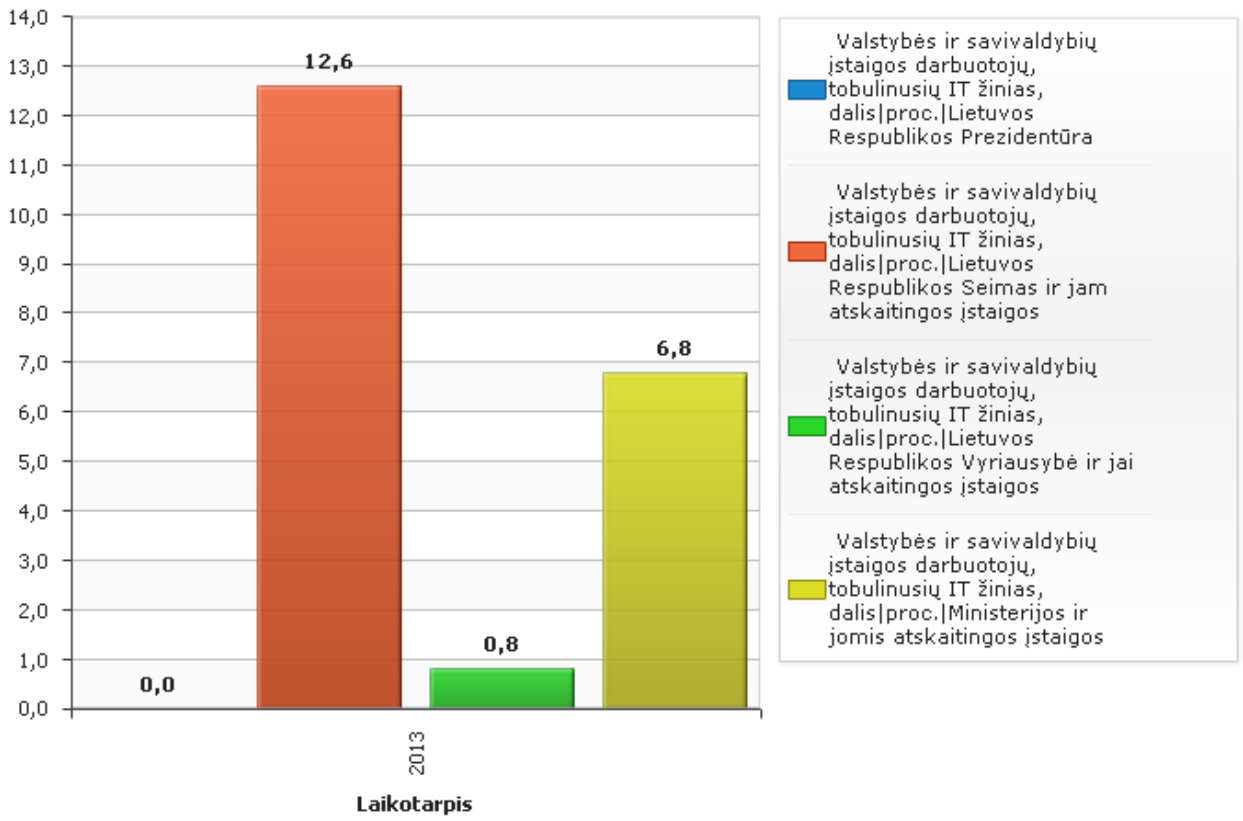
Situacija su teisėsaugos, teisėtvarkos ir muitinės įstaigomis panaši – didžioji dauguma darbuotojų, dirbdami kasdienius darbus susiduria su internetu. Teisėsaugos įstaigos – 93 proc., teisėtvarkos – 67,5 proc., muitinės įstaigos – 98,2 proc. Kiek mažiau, t. y. apie pusė įkalinimo įstaigos darbuotojų dirbdami naudojasi internetu (48 proc.), na, o mažiausiai darbe internetą naudoja priešgaisrinės apsaugos ir gelbėjimo įstaigos – 22, 6 proc.



Šaltinis: Lietuvos statistikos departamentas

Pav. 14 **Valstybės ir savivaldybių įstaigų (teisėsaugos, teisėtvarkos, muitinės, įkalinimo įstaigų ir priešgaisrinės apsaugos ir gelbėjimo įstaigų) darbuotojų, naudojančių internetą dalis**

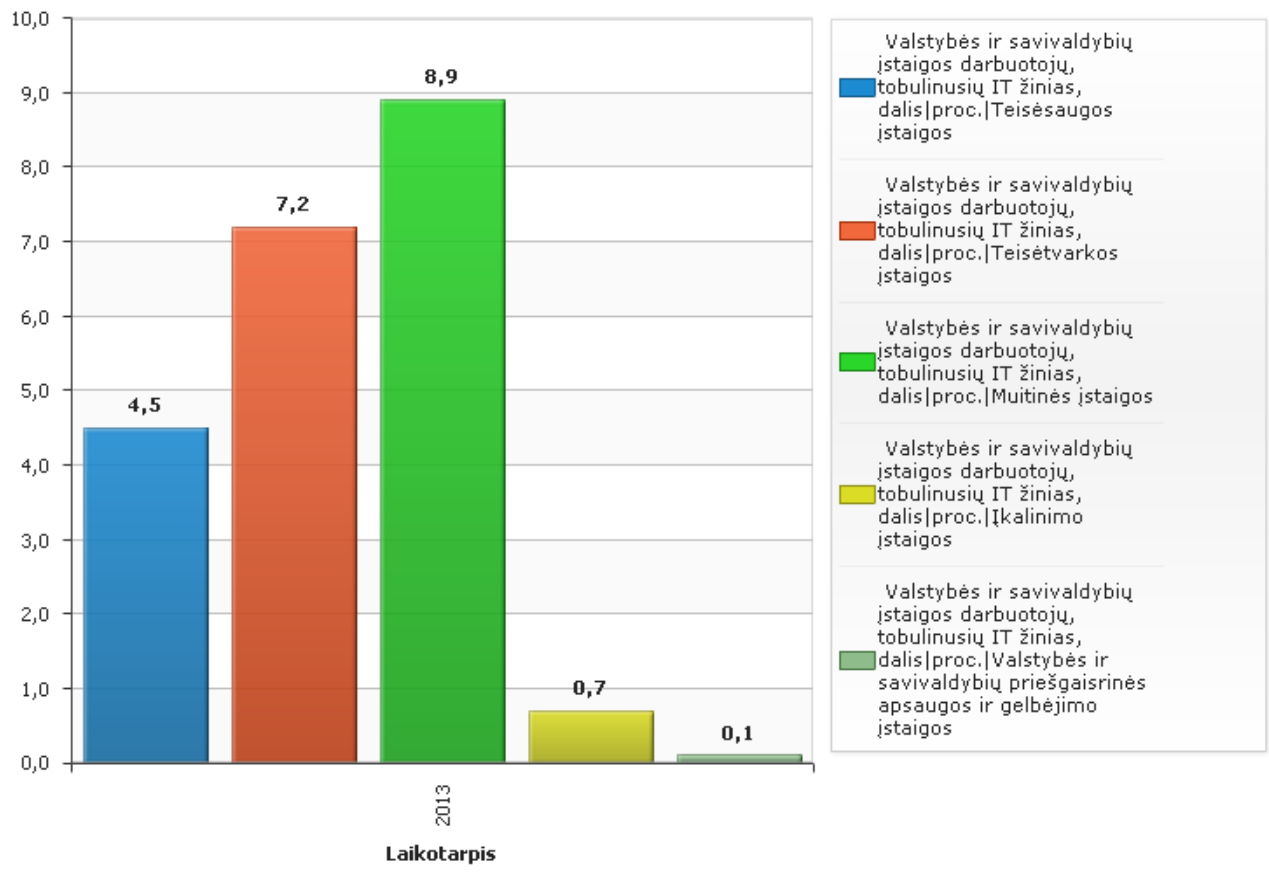
Nepaisant milžiniško interneto naudojimosi darbovietėse masto, darbuotojų, tobulinusių savo IT žinias dalis palyginti yra labai maža. 2013 m. LR Prezidentūros darbuotojai savo IT žinių iš viso netobulino (0 proc.), 0,8 proc. LR Vyriausybės ir jai atskaitingų įstaigų darbuotojų 2013 m. kėlė savo kvalifikaciją IT srityje, Ministerijose ir joms atskaitingose įstaigose IT žinias tobulinusių darbuotojų skaičius vos didesnis – 6,8 proc., na, o LR Seimo ir jam atskaitingų įstaigų darbuotojų 2013 m. tobulinusių IT žinias buvo 12,6 proc.



Šaltinis: Lietuvos statistikos departamentas

Pav. 15 **Valstybės ir savivaldybių įstaigų (LR Prezidentūros, LR Seimo ir jam atskaitingų įstaigų, LR Vyriausybės ir jai atskaitingų įstaigų, Ministerijų ir joms atskaitingų įstaigų) darbuotojų tobulinusių IT žinias dalis**

Kalbant apie teisėsaugos, teisėtvarkos, muitinės, įkalinimo bei priešgaisrinės apsaugos ir gelbėjimo įstaigų darbuotojų dalį, 2013 metais tobulinusią IT žinias situacija panaši – tik 0,1 proc. priešgaisrinės apsaugos ir gelbėjimo įstaigų darbuotojų gilino IT žinias, įkalinimo įstaigų darbuotojų – 0,7 proc. Teisėsaugos institucijų darbuotojai – 4,5 proc., teisėtvarkos – 7,2 proc. Kiek daugiau – 8,9 proc. Muitinės įstaigų darbuotojų 2013 metais tobulino IT žinias.



Šaltinis: Lietuvos statistikos departamentas

Pav. 16 **Valstybės ir savivaldybių įstaigų (teisėsaugos, teisėtvarkos, muitinės, įkalinimo įstaigų ir priešgaisrinės apsaugos ir gelbėjimo įstaigų) darbuotojų tobulinusių IT žinias dalis**

Nenuostabu, kad susiduriama su daugybe elektroninio saugumo problemų darbo vietose. Lietuvos kritinių infrastruktūrų darbuotojai, naudodamiesi internetinėmis technologijomis kiekvieną dieną, savo žinias tobulina minimaliai. Elektroniniai incidentai, gali būti darbuotojų kompetencijos, dirbant su IT, trūkumo priežastys.

2. Aukos, aptikusios kompiuterinius nusikaltimus vengia apie juos kalbėti. Pasak M. Kiškio, verslo sektoriuje šis nenoras yra susijęs su dviem dalykais:

- Kai kurios aukos nenori atskleisti informacijos apie savo darbą bijodamos viešumo arba bijo sugadintos reputacijos;
- Kitos aukos bijo prarasti investuotoją arba visuomenės pasitikėjimą.

Apskaičiuoti kibernetinių nusikaltimų žalą yra labai sunku, nes nusikaltimų padarinių šalinimas dažnai nėra vien tik skaitmeninių duomenų atstatymas, ar neteisėtai pasisavintų pinigų grąžinimas UNOCD (United Nations Office on Drugs and Crime) duomenimis.

Lietuvos Respublikos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio CERT-LT , 2014 metais buvo ištirta 36 136 incidentų pagal pranešimus,

gautus iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus ir iš Lietuvos interneto naudotojų. Lyginant su 2013 metais (25 337), kibernetinių incidentų skaičius Lietuvoje išaugo 43 proc.

2014 metais buvo užfiksuoti net 13 827 incidentai susiję su fiziniams asmenims priklausančiais įrenginiais kurie turėjo saugumo spragų. Tai išties didelė problema, nes nusikaltėliai pasinaudoję aukų įrenginiais gali sukelti DDos (angl. *Distributed Denial of Service*) atakas. DDos - paskirstyto atsisakymo aptarnauti atakos.

Užfiksuota ir ištirta nemažai incidentų (11 276), kurie yra susiję su kenksminga programine įranga. Kenksminga programinė įranga yra naudojama kai nusikaltėliai siekia kompiuterius įtraukti į botnet tinklą. Dažniausiai kenkimo programinė įranga naudojama siekiant naudotojų kompiuterius įtraukti į botnet tinklą. Tai tokie tinklai, kurie sudaromi užkrėtus daug kompiuterių ir vėliau juos panaudojant įvairioms, dažniausiai paskirstyto atsisakymo aptarnauti (*DDos*), atakoms vykdyti. Auka ilgą laiko net nežino, kad jos kompiuteris yra įtrauktas į botnet tinklą, nes kompiuteris veikia normaliai, tiesiog retkarčiais gali sulėtėti interneto ryšys. Pasak CERT-LT, 2015 metais kenksmingos programinės įrangos kūrėjai dar labiau sieks užkrėsti kuo daugiau išmaniųjų telefonų ir plančetinių kompiuterių.

2014 metais buvo gauti ir ištirti 165 pranešimai apie paslaugos trikdymo atakas (angl. *Denial of Service, DoS*). Atakos metu maži 8 baitų UDP paketai su falsifikuotu IP adresu yra pradedami siųsti į pažeidžiamą NTP serverį. Savo ruožtu serveris į kiekvieną paketą atsako daug didesniais atsakymais, rezultate įgyvendinama DoS ataka. Šios atakos dažniausiai yra vykdomos pasitelkus botnet tinkle resursus. Lyginant su 2013 metais, atakų skaičius išaugo 27 proc. Tam, kad DoS atakų būtų kuo mažiau, CERT-LT elektroninių svetainių savininkams ir elektroninės informacijos prieglobos paslaugas teikiančioms įmonėms pateikė rekomendacijas bei metodus, kaip būtų nuo minėtų atakų apsisaugoti.

CERT-LT ištyrė 630 incidentus susijusius su klastojimu (angl. *phishing*). Phishing'u yra vadinamas internetinių svetainių klastojimas, siekiant gauti internetinių paskyrų duomenis ir iš to išpešti finansinės naudos. Dažniausiai tai būna suklastoti elektroninių mokėjimo sistemų puslapiai (pavyzdžiui PayPall). Atsitinka ir taip, kad susiduriama su suklastotais populiarių socialinių tinklų, tokių kaip Facebook, Gmail, Yahoo interneto puslapiais.

2014 metais, lyginant su 2013 metais informacinių sistemų užvaldymo incidentų sumažėjo maždaug 50 proc. 2013 metais incidentų buvo 10 924, 2014 m. informacinių sistemų užvaldymo atvejų sumažėjo iki 4 853. Šie rezultatai pasiekti dėka CERT-LT veiksmų tobulinant reagavimo priemones. CERT-LT ištyrė, kad dauguma informacinių sistemų užvaldymo atvejų buvo

atlikti automatizuotai – pasitelkiant jau minėtus botnet tinklus ir į silpnai apsaugotas interneto svetaines įterpus kenksmingą kodą.

Milžiniški informacijos kiekiai yra saugomi privačių įmonių duomenų centruose, valstybės institucijų duomenų bazėse ir informacinių sistemų duomenų saugyklose. „Tokios informacijos paviešinimas, nesavalaikis panaudojimas ar sugadinimas gali sukelti didžiules problemas ir ženklius piniginius nuostolius verslo organizacijoms ar viešojo administravimo subjektams“ (Štitilis, 2014).

Akivaizdu, kad kibernetinių incidentų skaičius Lietuvoje, kaip ir visame pasaulyje auga ir kibernetinio saugumo problema kelia vis didesnių rūpesčių. Todėl yra būtina reaguoti ir imtis veiksmų siekiant sumažinti incidentų skaičių iki minimumo.

2012 m. birželio 26 d. buvo atnaujinta Lietuvos Respublikos Nacionalinio saugumo strategija (Lietuvos Respublikos nutarimas, Dėl nacionalinio saugumo strategijos patvirtinimo, 2002 m. gegužės 28 d). Joje buvo išskirti nacionalinio saugumo interesai, tarp jų – kibernetinis saugumas, taip pat išskirtos naujos grėsmės, tokios kaip kibernetinės atakos – elektroninių ryšių tinklų ir informacinių sistemų atakos, kuriomis siekiama sutrikdyti nacionaliniam saugumui strategiškai svarbių ūkio sektorių infrastruktūros funkcionavimą ir nacionaliniam saugumui svarbių valstybės institucijų veiklą, išgauti įslaptintą informaciją, vykdyti kitas nusikalstamas veikas ir taip pakenkti valstybės ir jos piliečių saugumui.

Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos parengtoje ataskaitoje (už 2013 metus), akcentuojama, kad pavojingą veiklą kibernetinėje erdvėje (žvalgybinį skenavimą, kibernetines atakas ir t.t.) nukreiptas prieš Lietuvą galėjo lemti šie veiksniai:

- Kibernetinio saugumo įstatymo bei efektyviai veikiančios institucijos, kuri būtų atsakinga už kibernetinį saugumą nebuvimas;
- Lengvabūdiškas ar neatsakingas elgesys dirbant su Lietuvos valstybės institucijų automatizuoto duomenų apdorojimo sistemomis ir tinklais.

Siekiant gerinti šią situaciją Lietuva aktyviai ėmėsi veiksmų 2014 m. gruodžio 11 d. Lietuvoje buvo paskelbtas Kibernetinio saugumo įstatymas (įsigaliojo nuo 2015 m. sausio 1 d.). Kartu su įstatymo įsigaliojimu savo veiklą pradėjo Nacionalinis kibernetinio saugumo centras (institucija atsakinga už kibernetinį saugumą), kurio funkcijos pagal įstatymą yra:

- *pagal savo kompetenciją rengti ir teikti pasiūlymus krašto apsaugos ministrui dėl organizacinių ir techninių kibernetinio saugumo reikalavimų valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai;*
- *atlikti valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams stebėseną;*

- *rengti tipinius kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus;*
- *teikti konsultacijas ir rekomendacijas valstybės informacinių išteklių valdytojams ir ypatingos svarbos infrastruktūros valdytojams kibernetinio saugumo klausimais;*
- *analizuoti nacionalinę kibernetinio saugumo situaciją ir rengti nacionalinio kibernetinio saugumo būklės ataskaitas;*
- *ne rečiau kaip kartą per metus rengti ir teikti nacionalinio kibernetinio saugumo būklės ataskaitas krašto apsaugos ministrui;*
- *rengti ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus;*
- *valdyti kibernetinio saugumo informacinį tinklą;*
- *vykdyti informacijos sklaidą kibernetinio saugumo klausimais;*
- *laikantis krašto apsaugos ministro nustatytos tvarkos, reaguoti į kibernetinius incidentus valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose;*
- *atlikti kitas Lietuvos Respublikos teisės aktuose nustatytas funkcijas kibernetinio saugumo užtikrinimo srityje.* (Lietuvos Respublikos kibernetini saugumo įstatymas, 2014).

1.9 Kibernetinio saugumo plėtros 2011 – 2019 metais programa

Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“ buvo patvirtinta Kibernetinio saugumo plėtros programa 2011–2019 metams.

Ši programa buvo parengta atsižvelgiant į tai, kad valstybės ir visuomenės gyvenime vis didesnę reikšmę įgyja informacinėmis ir ryšių technologijomis tvarkoma ir perduodama elektroninė informacija, atsiradusios elektroninės informacijos tvarkymo galimybės paskatino nacionalinių ir globalių informacinių visuomenių atsiradimą ir sudarė sąlygas toliau modernizuoti šalių ūkius ir efektyviau valdyti valstybę, tačiau tuo pačiu metu į elektroninę formą perkeliama vis daugiau informacijos, sparčiai automatizuojami įvairūs šalies valdymo ir ūkio veiklos procesai, globali kibernetinė erdvė ir joje teikiamos viešosios paslaugos tapo patraukliu atskirų asmenų, nusikalstamų grupuočių, politinių jėgų ir kitų subjektų taikiniu (Lietuvos Respublikos vyriausybės 2011 metų birželio 29 dienos nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“, 2011).

Programos paskirtis buvo nustatyti kibernetinio saugumo plėtros tikslus ir uždavinius, tam, kad būtų užtikrintas elektroninės informacijos konfidencialumas, vientisumas ir prieinamumas, informacinių sistemų, elektroninių ryšių tinklų ir ypatingos svarbos informacinės infrastruktūros (dar vadinamos kritine infrastruktūra) bei privačių asmenų apsauga nuo incidentų ir kibernetinių atakų.

Strateginis programos tikslas yra „plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus 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 Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis pasiektų 60 procentų“ (Lietuvos Respublikos vyriausybės 2011 metų birželio 29 dienos nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo, 2011).

Įgyvendinimo tikslai

Kibernetinio saugumo plėtros programoje nustatyti įgyvendinimo tikslai:

1. **Pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas.** Programoje pažymėta, kad nėra sukurta elektroninės informacijos saugos valdymo koordinavimo sistema (išskyrus valstybinį sektorių, t. y. Lietuvos Respublikos Vyriausybei atskaitingas įstaigas ir institucijas). Trūksta įgaliojimų vykdyti kibernetinio saugumo kontrolę ir koordinavimą. Reikalingas Lietuvos viešojo ir privataus sektoriaus subjektų bendradarbiavimas, o jo trūkumas neleidžia veiksmingai planuoti elektroninės kibernetinio saugumo srities plėtros. Bendradarbiavimo spragos sudaro sąlygas sutrikdyti informacinių išteklių, taip pat ypatingos svarbos informacinės infrastruktūros objektų funkcionavimą, o šių pažeidžiamumų aptikimo ir šalinimo veiksmingumas didėja centralizuojant šią veiklą. Kibernetinių incidentų skaičius auga, o didelio masto incidentai kibernetinėje erdvėje gali sukelti nacionalinio saugumo krizę. Šiam tikslui pasiekti būtina išspręsti šiuos uždavinius:

- reglamentuoti elektroninės informacijos saugą;
- tobulinti kibernetinio saugumo kontrolę ir koordinavimą;
- užtikrinti interneto ir kitų informacinės infrastruktūros paslaugų teikėjų teikiamų paslaugų saugumą;
- užtikrinti patikimą tapatybės nustatymą, kas sumažintų didelę dalį grėsmių, susijusių su kibernetine erdve, o tai skatintų naudotojų pasitikėjimą kibernetine erdve;
- aukštos kompetencijos specialistų bendradarbiavimas, keitimasis turima informacija ir patirtimi yra būtina veiksmingos išankstinio perspėjimo ir prevencinės veiklos sąlyga;
- plėtoti saugią valstybės informacinę infrastruktūrą;
- skatinti elektroninės informacijos saugos (kibernetinio saugumo) projektų įgyvendinimą;
- plėtoti tarptautinį bendradarbiavimą kibernetinio saugumo srityje.

Kalbant apie kibernetinio saugumo valdymo koordinavimo sistemą, galima teigti, jog pirmi žingsniai jau žengti. LR kibernetinio saugumo įstatymas nurodo, kad kibernetinio saugumo politiką formuoja, koordinuoja ir jos įgyvendinimą organizuoja LR Krašto apsaugos ministerija. Kitos įstatyme išvardintos institucijos padeda vykdyti politiką pagal turimas kompetencijas.

Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų tiekėjai ir elektroninės informacijos prieglobos paslaugų tiekėjai bendradarbiauja su Ryšių reguliavimo tarnyba ir teikia jai visą informaciją apie įvykusius kibernetinius incidentus. Pagal incidentų specifiką toliau gali būti kreipiamasi į Valstybinę duomenų apsaugos inspekciją ir Policijos departamentą. Taip pat, tyrimus, susijusius su Lietuvos ūkio subjektais, teikiančiais viešuosius ryšių tinklus, viešąsias elektroninių ryšių paslaugas ir (ar) informacinės visuomenės tarpines paslaugas, teikiamas viešaisiais ryšių tinklais atlikti padeda CERT-LT.

Dėl aukštos kompetencijos specialistų bendradarbiavimo ir keitimosi naudinga informacija bei tarptautinio bendradarbiavimo, galima būtų pabrėžti, kad „2010 m. Krašto apsaugos ministerija ir NATO Kibernetinės gynybos valdymo agentūra pasirašė dvišalį susitarimą dėl bendradarbiavimo kibernetinės gynybos srityje. Šiuo susitarimu siekiama pagerinti nacionalinių kibernetinės gynybos pajėgumų vystymą, sustiprinti bendradarbiavimą tarp Krašto apsaugos ministerijos ir NATO kibernetinės gynybos valdymo agentūros ir pagerinti kibernetinių atakų prognozavimo, aptikimo ir atsako į jas pajėgumus. Susitarime taip pat numatoma, kad, kibernetinės atakos atveju, Krašto apsaugos ministerija gali kreiptis į NATO Kibernetinės gynybos valdymo agentūrą prašydama atsiųsti NATO greitojo reagavimo kibernetinės gynybos specialistų komandą. Lietuva dalyvauja NATO Bendros kibernetinės gynybos kompetencijos centro, kuris įsikūręs Estijoje, veikloje. Šio centro veikloje taip pat dalyvauja Estija, Latvija, Lenkija, Vokietija, Italija, Vengrija, Slovakija, Ispanija, Nyderlandai ir JAV“ (Kibernetinė gynyba ir energetinis saugumas, 2014).

Kalbant apie privataus ir viešojo sektoriaus bendradarbiavimą – nėra tiksliai įvardinta, kokiomis priemonėmis jis turėtų būti užtikrinamas, nėra reglamentuojama kaip tokį bendradarbiavimą reiktų skatinti.

Būtina sukurti teisinę bazę, kuri reglamentuotų tapatybės nustatymo priemonių panaudojimą, tokiu būdu būtų išvengta tapatybės vagystės atvejų. Patikimos tapatybės nustatymo priemonės užtikrintų rizikos sumažėjimą, skatintų vartotojų pasitikėjimą kibernetine erdve.

2. **Užtikrinti veiksmingą ypatingos svarbos informacinės infrastruktūros funkcionavimą**. Kritinės svarbos informacinės infrastruktūros saugumas užtikrinamas tik žinybiniu lygmeniu, nesuformuota koordinavimo struktūra, neišanalizuoti šios infrastruktūros objektų tarpusavio ryšiai ir sutrikdymo poveikis nacionaliniu mastu, nevykdomas veiklos tęstinumo planavimas. Tam, kad būtų įsitikinta kritinės infrastruktūros sistemų saugumu būtina išspręsti šiuos uždavinius:

- vykdyti įsilaužimo į sistemas pratybas (testavimą) (angl. – *penetration test*) ir patikrinti, ar tinkamai veikia apsaugos sistema;
- vykdyti stebėseną kaip prevencijos priemonę.

Pagal LR kibernetinio saugumo įstatymą, už ypatingos svarbos informacinės infrastruktūros saugumą yra atsakingas Nacionalinis kibernetinio saugumo centras. Tačiau Lietuvoje ypatingos svarbos informacinė infrastruktūra šiuo metu nėra identifikuota. Remiantis užsienio saugumo ekspertų patirtimi kritinėmis infrastruktūromis reiktų laikyti:

- energetikos sektorių;
- finansines ir draudimo institucijas;
- telekomunikacijų operatorius;
- interneto paslaugų tiekėjus;
- sveikatos apsaugos institucijas;
- transporto sektorių;
- oro transportą;
- karines struktūras ir priemones;
- Valstybines paslaugas;
- Vandentiekio ir nuotekų šalinimo sistemas;
- Maisto gamybos segmentas;
- Pagrindiniai internetiniai portalai bei televizija.

3. **Siekti užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje.** Šiuo metu ne visi elektroninės informacijos naudotojai rūpinasi elektroninės informacijos sauga. Siekiant to išvengti būtina išspręsti šiuos uždavinius:

- teikti bazines elektroninės informacijos saugos žinias ir įrankius, kurie leistų naudotojams išvengti grėsmių kibernetinėje erdvėje (plėtoti kibernetinio saugumo kultūrą);
- stiprinti kibernetinėje erdvėje teikiamų paslaugų saugumą;
- Plėtoti nenutrūkstamai veikiančią ir tinkamai valdomą sistemą, apimančią visą incidentų gyvavimo ciklą: išankstinio perspėjimo, prevencijos, aptikimo, likvidavimo ir tyrimo fazes;
- blokuoti interneto prieigą kenkėjišką veiklą vykdantiems asmenims ir (ar) įrenginiams (šiuo metu visuomenėje yra susiformavęs stereotipas dėl nebaudžiamumo už neteisėtus veiksmus kibernetinėje erdvėje, todėl svarbu šį stereotipą panaikinti);
- kibernetinės atakos, kurių šaltinis yra užsienyje, gali ir turi būti stabdomos ties virtualiu Lietuvos kibernetinės erdvės perimetru, siekiant išvengti jų poveikio šalies vidaus elektroninių ryšių tinkluose.

Visų pirma, siekiant užtikrinti Lietuvos žmonių ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje būtina ugdyti supratimą apie kibernetinėje erdvėje tykančius pavojus. Tam padėtų švietimas kibernetinio srityje, kuris galėtų būti ugdomas mokyklose, darbo vietose. Pagal dabartinę statistiką, valstybinių institucijų darbuotojų švietimas kompiuterinių technologijų srityje, o

taip pat ir kompiuterio saugumo srityje yra menkas. Privatusis sektorius taip pat nelinkęs daug investuoti nei į darbuotojų apmokymus, nei į elektronines duomenų apsaugos programas.

Pagal LR kibernetinio saugumo įstatymą, tiek NKSC tiek ir elektroninių viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų bei elektroninės informacijos prieglobos paslaugų tiekėjai privalo teikti paslaugų gavėjams rekomendacijas apie priemones kibernetiniam saugumui užtikrinti naudojantis teikiamomis paslaugomis. Tačiau, kol nebus suformuota „kibernetinio saugumo kultūra“ ir vartotojai patys nesupras rizikos, su kuria susiduria, šios rekomendacijos gali būti bevertės.

Lietuvoje trūksta teisinio reglamentavimo, kuris apibrėžtų testavimo priemonių taikymą kritinėse infrastruktūrose (angl. *penetration test*). Bandymų įsilaužti į kritines sistemas būdas padėtų įsitikinti, ar tinkamai veikia saugumo sistemos ir būtų lengviau pastebėti kurias sritis būtina stiprinti. Šiuo metu stebėsena ir incidentų prevencija kritinėse infrastruktūrose užsiima Nacionalinis kibernetinio saugumo centras.

Programos įgyvendinimas . Pasak Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimo Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“ programos įgyvendinimą koordinuoja Vidaus reikalų ministerija, tačiau kibernetinio saugumo įstatyme apibrėžta, kad „Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija“. Taigi, iškyla neatitikimas dėl teisingo supratimo, kas vis dėl to formuoja ir koordinuoja kibernetinio saugumo politiką šalyje.

1.10 Lietuvos Respublikos kibernetinio saugumo įstatymas

2014 m. gruodžio 11 d. Lietuvoje paskelbtas Kibernetinio saugumo įstatymas (įsigaliojo nuo 2015 m. sausio 1 d.). Šio įstatymo pagrindinis paskirtis yra „nustatyti kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžti kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų kompetenciją, funkcijas, teises ir pareigas, valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų pareigas bei atsakomybę ir kibernetinio saugumo užtikrinimo priemones“ (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014). Įstatymas yra taikomas „valstybės institucijoms, formuojančioms ir įgyvendinančioms kibernetinio saugumo politiką, viešojo administravimo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams ir elektroninės informacijos prieglobos paslaugų teikėjams, informacinių technologijų srityje veiklą vykdantiems verslo subjektams, mokslo ir studijų institucijoms „Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

Šis įstatymo įgyvendinimas yra vienas iš Kibernetinio saugumo plėtros programos 2011–2019 metams tikslų (pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas).

Lietuvos Respublikos kibernetinio saugumo įstatyme kibernetinis saugumas grindžiamas bendraisiais teisės principais, elektroninių ryšių veiklos reguliavimo principais bei šiais principais:

1. **kibernetinės erdvės nediskriminavimo** – įstatymų ir kitų teisės aktų nuostatos turi būti taikomi tiek fizinėje, tiek elektroninėje erdvėje;
2. **kibernetinio saugumo proporcingumo** – priemonės naudojamos užtikrinti kibernetinį saugumą negali būti griežtesnės nei būtina. Taip pat, taikomi teisiniai, organizaciniai ir techniniai kibernetinio saugumo reikalavimai neturi apriboti kibernetinio saugumo dalyvių veiklos kibernetinėje erdvėje labiau, negu tai būtina;
3. **viešojo intereso viršenybės** – naudojamos kibernetinio saugumo užtikrinimo priemonės pirmiausia turi užtikrinti visuomenės viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų teisių ar neproporcingai apriboti jų laisvės kibernetinėje erdvėje.

Pagal šį įstatymą Lietuvos Respublikos Vyriausybė nustato strateginius ir priemones jiems pasiekti. Lietuvos Respublikos Krašto apsaugos ministerija yra institucija, kuri formuoja kibernetinio saugumo politiką, organizuoja, kontroliuoja ir koordinuoja jos įgyvendinimą.

„Kitos įstatyme paminėtos institucijos, tokios kaip Lietuvos Respublikos vidaus reikalų ministerija, Nacionalinis kibernetinio saugumo centras, Lietuvos Respublikos ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija ir Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek šiame įstatyme nustatytoms funkcijoms atlikti reikia nustatyti viešojo administravimo subjektų, valdančių valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veiklos teisinį reguliavimą“ (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

Pagal kompetenciją, kibernetinio saugumo politiką įgyvendina Vidaus reikalų ministerija, Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija ir Policijos departamentas. Lentelėje pateikta kibernetinio saugumo politikos formavimo ir įgyvendinimas schema.

lentelė 5 Lietuvos institucijų, vykdančių kibernetinio saugumo užtikrinimą veiklos sritys ir funkcijos

<table>
<tr><td colspan="5">Lietuvos Respublikos Vyriausybė
Formuoja strateginius tikslus ir priemones;
Steigia Kibernetinio saugumo Tarybą;
Tvirtina planus;
Sudaro Kibernetinio saugumo tarybą, kurią sudaro:
Politiką formuojančių ir įgyvendinančių institucijų nariai, IT verslo atstovai, mokslo ir akademinės bendruomenės atstovai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų atstovai ir kt. Tarybai vadovauja KAM atstovas.
Taryba analizuoja kibernetinio užtikrinimo būklę Lietuvoje ir teikia pasiūlymus dėl būklės gerinimo.</td></tr>
<tr><td colspan="5">Lietuvos Respublikos krašto apsaugos ministerija
Formuoja kibernetinio saugumo politiką ;
Organizuoja, kontroliuoja, koordinuoja politikos įgyvendinimą</td></tr>
<tr><td>Vidaus reikalų ministerija (VRM)
Įgyvendina politiką pagal kompetenciją;
Rengia ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką ir (arba) ypatingos svarbos informacinės infrastruktūros valdytojų sąrašą.</td><td>Nacionalinis kibernetinio saugumo centras (NKSC)
Įgyvendina politiką pagal kompetencijas;
Reaguoja į su valstybės informaciniais ištekliais ir ypatingos svarbos informacine infrastruktūra susijusius kibernetinius incidentus.
Turi teisę duoti nurodymus viešųjų ryšių tinklų ir (arba) viešųjų elektroninių paslaugų tiekėjams apriboti paslaugų tiekimą (nors nurodymus paprastai duoda Ryšių reguliavimo tarnyba);</td><td>Ryšių reguliavimo tarnyba (RRT)
Duoda nurodymus ryšių tiekėjams.</td><td>Valstybinė duomenų apsaugos inspekcija (VDAI)
Tikrina juridinius asmenis;
Teikia visuomenei informaciją susijusią su asmens duomenų apsauga;
Teikia informaciją institucijoms susijusią su asmens duomenų apsauga.</td><td>Policijos departamentas (PD)
Dirba su incidentais, galimai turinčiais nusikalstamos veikos požymių;
Turi teisę apriboti prieigą prie elektrinės informacijos prieglobos paslaugų, kai asmuo arba turima įranga galimai dalyvauja nusikalstamoje veikoje.
Turi teisę prašyti duomenų apie asmenis iš elektrinės informacijos prieglobos paslaugų.</td></tr>
</table>

	• Skelbia visuomenei informaciją ir rekomendacijas dėl kibernetinių incidentų.			

Sudaryta autoriaus pagal LR Kibernetinio saugumo įstatymą.

Įstatyme apibrėžtos kibernetinio saugumo dalyvių pareigos:

- **Viešojo administravimo subjektai**: atsako už valstybės informacinių išteklių saugumą; informuoja NKSC, VDAI arba policijai apie incidentus susijusius su jų valdomais arba tvarkomais informaciniais ištekliais; paskiria kompetentingą asmenį, arba padalinį, kuris būtų atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą, o taip pat pateikia NKSC jo kontaktinius duomenis.
- **Ypatingos svarbos informacinės infrastruktūros objektai**: atsako už jų valdomų infrastruktūros saugumą; informuoja NKSC, VDAI arba policijai apie incidentus apibrėžtus organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose; teikia NKSC kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus; išbando kibernetinių incidentų planų veikimą ir bandymų rezultatus pateikia NKSC; paskiria kompetentingą asmenį, arba padalinį, kuris būtų atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą, o taip pat pateikia NKSC jo kontaktinius duomenis.
- **Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų tiekėjai**: skelbia paslaugų gavėjams informaciją bei priemones siekiant užtikrinti kibernetinį saugumą; teikia informaciją RRT, VDAI arba policijai apie kibernetinius incidentus bei teikia reikalingą techninę informaciją; paskiria kompetentingą asmenį, arba padalinį, kuris būtų atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą, o taip pat pateikia RRT jo kontaktinius duomenis.
- **Elektroninės informacijos prieglobos paslaugų tiekėjai**: privalo įgyvendinti kibernetinio saugumo priemones, kurias nustatyto RRT; viešai skelbti paslaugų gavėjams rekomendacijas bei priemones saugumui užtikrinti; teikia informaciją RRT ir policijai apie kibernetinius incidentus; privalo įvykdyti policijos nurodymus dėl paslaugų teikimo gavėjui apribojimo; paskiria kompetentingą asmenį, arba padalinį, kuris būtų atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą, o taip pat pateikia RRT jo kontaktinius duomenis.

Tarpinstitucinis bendradarbiavimas

Pagal Lietuvos Respublikos kibernetinio saugumo įstatymo nuostatas Kibernetinio saugumo informacinį tinklą valdo Nacionalinis kibernetinio saugumo centras. Nacionalinis kibernetinio saugumo centras yra patikima informacijos mainų platforma, kurios pagrindinis tikslas

yra informacijos apie kibernetinius incidentus dalijimasis, o taip pat bendradarbiavimas tarp kibernetinio saugumo informacinio tinklo narių. Subjektai, kurie atitinka Kibernetinio saugumo informacinio tinklo nuostatuose nurodytus reikalavimus gali naudotis informaciniu tinklu ir gauti aktualią informaciją apie kibernetinius incidentus, taip pat kitų subjektų, atsakingų už kibernetinio saugumo organizavimą ir kibernetinių incidentų valdymą kontaktinę informaciją.

„Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Policijos departamentas ir kitos policijos įstaigos bendradarbiauja tiriant kibernetinius incidentus, keičiasi su kibernetinių incidentų tyrimais susijusia informacija, kuri reikalinga tyrimams atlikti. Valstybinė duomenų apsaugos inspekcija bendradarbiauja su Nacionalinio kibernetinio saugumo centru ir Ryšių reguliavimo tarnyba tiriant kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, keičiasi informacija, reikalinga teisės aktų nustatytoms funkcijoms, susijusioms su kibernetinių incidentų, pažeidžiančių asmens duomenų saugumą, tyrimu, atlikti“ (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

KIBERNETINIO SAUGUMO UŽTIKRINIMO LIETUVOJE TYRIMAS

1.11 Tyrimo metodologija

Tyrimo problema. Mokslo šaltiniuose nepakankamai išanalizuoti kibernetini saugumo užtikrinimo metodai ir tiksliai neapibrėžtas teisinis reguliavimas gali lemti kibernetinio saugumo stoką Lietuvoje.

Tyrimo objektas. Kibernetinio saugumo situacija ir perspektyva Lietuvoje.

Tyrimo tikslas. Nustatyti, kaip kibernetinio saugumo ekspertai vertina kibernetinio saugumo situaciją ir perspektyvą Lietuvoje.

Empirinio tyrimo uždaviniai:

- Atlikti ekspertų nuomonės tyrimą, kuris padėtų išsiaiškinti požiūrį į kibernetinio saugumo situaciją ir perspektyvas Lietuvoje.
- Pasiūlyti alternatyvius kibernetinio saugumo užtikrinimo Lietuvoje metodus ir priemones.

Tyrimui atlikti buvo pasirinktas kokybinis tyrimo metodas – ekspertinis interviu. „Ekspertas – asmuo, kuris dėl savo profesinės arba gyvenimo patirties turi didžiausią kompetenciją ir patikimiausią bei pakankamai išsamią informaciją apie tiriamą problemą“ (Tidikis, 2003). Ekspertinės informacijos gavimui buvo pasirinktas formalaus interviu būdas. Interviu buvo vykdomas pagal iš anksto suformuluotus klausimus. Ši forma pasirinkta siekiant gauti informaciją, kurią būtų galima palyginti ir analizuoti.

Klausimyno sudarymas. Tyrimui atlikti buvo parengtas klausimynas iš 10 klausimų. Klausimų tipas – atviri klausimai. Interviu metu buvo pateikti klausimai (žr. lentelę 6). Pažymėta, jog klausimynu siekiama išsiaiškinti ekspertų požiūrį į kibernetinio saugumo situaciją Lietuvoje.

lentelė 6 Klausimynas

1. Kokia, Jūsų nuomone, šiuo metu yra didžiausia problema Lietuvoje susijusi su kibernetiniu saugumu?
2. Kuris sektorius Lietuvoje, Jūsų nuomone, geriau susitvarko su kibernetinio saugumo problemomis? Privatusis ar valstybinis? Kodėl?
3. Kaip manote, ar Lietuvos teisinė bazė yra pakankama siekiant užtikrinti operatyvų institucijų, atsakingų už kibernetinio saugumo užtikrinimą, bendradarbiavimą? Ir ar šių institucijų funkcijos yra aiškiai ir pakankamai apibrėžtos?
4. Lietuvos Respublikos Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 programoje buvo iškeltas strateginis tikslas – „plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus 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 Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis pasiektų 60 procentų“. Kaip manote, ar Lietuva sėkmingai eina link šio strateginio tikslo įgyvendinimo?

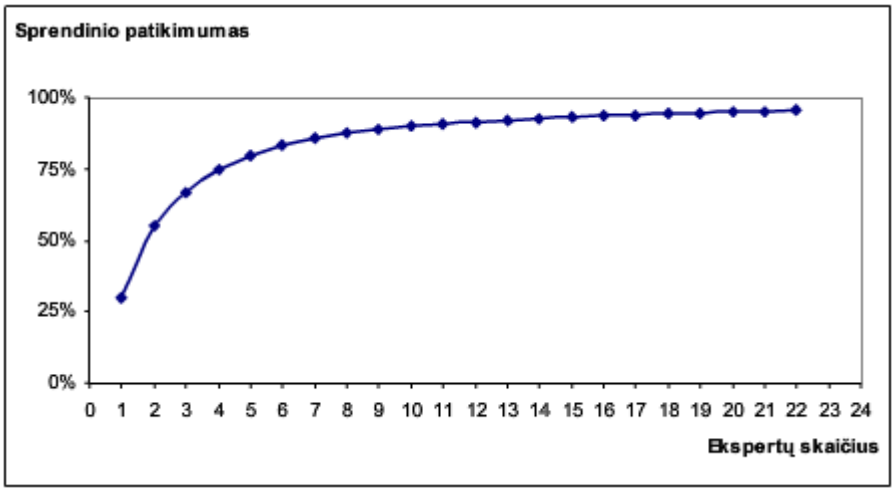
5. Šių metų pradžioje turėjo būti sudarytas ypatingos svarbos informacinės infrastruktūros sąrašas. Į jį patektų valstybės ir privačių įmonių valdomos informacinės sistemos, kurias pažeidus per kibernetines atakas gali kilti grėsmė visos Lietuvos visuomenės saugumui ar valstybės interesams. Kokie sektoriai patenka į šį sąrašą?
6. Kibernetinio saugumo įstatyme apibrėžta, kad Nacionalinis kibernetinio saugumo centras (NKSC) vykdo tik valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros apsaugą ir prevenciją. Kas tuo tarpu atsakingas už privačiojo sektoriaus saugumą? Į ką turėtų kreiptis paprastas Lietuvos pilietis patyręs kibernetinį incidentą? Į elektroninės informacijos prieglobos paslaugų tiekėją, Ryšių reguliavimo tarnybą ar policiją?
7. Ar ruošiant LR Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programą bei LR Kibernetinio saugumo įstatymą buvo remtasi užsienio valstybių praktika? Jei taip, kokios tai valstybės?
8. Jūsų nuomone, kaip Lietuva atrodo kibernetinio saugumo kontekste ES ir NATO šalių mastu?
9. Kada galima tikėtis sulaukti Lietuvos kibernetinio saugumo strategijos? Kokių ES ir NATO šalių gerosiomis praktikomis bus remiamasi formuojant Lietuvos kibernetinio saugumo strategiją?
10. Ar Lietuvoje vykdomos kibernetinio saugumo pratybos? Ar pratybos galėtų būti naudojamos kaip metodas padedantis užtikrinti kibernetinio saugumą Lietuvoje?

Sudaryta autoriaus

1.12 Tyrimo respondentų charakteristika

Tyrime dalyvaujančių ekspertų grupės dydis priklauso nuo jų kvalifikacijos dydžio. „Sunku (ir nebūtina) surinkti didesnę grupę aukščiausios kvalifikacijos ekspertų, nes specialistų, galinčių užginčyti ar paneigti jų nuomonę, negali būti daug. Siekiant išlaikyti ekspertinio vertinimo tikslumą ir patikimumą rekomenduojama įtraukti ne mažiau kaip 5 ekspertus“ (Augustinaitis, 2009).

Siekiant nustatyti priimtiną ekspertų kiekį būtina atsižvelgti į prielaidas, kurias suformulavo klasikinė testų teorija. Ši teorija teigia, kad agreguotų sprendimų patikimumą ir priimančiųjų (ekspertų) sprendimą skaičių sieja greitai slopstantis netiesinis ryšys (Brock, Hommes, 1997) (žr. Pav. 17).



Šaltinis: (Augustinaitis ir kt., 2009).

Pav. 17 **Ekspertų skaičiaus įtaka vertinimo patikimumui**

Taigi, tyrimui atlikti buvo pasirinkti 5 kibernetinio saugumo ekspertai. Norint išlaikyti konfidencialumą, ekspertams suteikiami kodai (arabiški skaitmenys nuo 1 iki 5) anonimiškumui garantuoti.

Formuluojant tyrimo klausimus buvo siekiama išsiaiškinti tiek viešojo, tiek privataus sektoriaus ekspertų nuomonę kibernetinio saugumo srityje, todėl dalyvauti tyrime buvo pakviesti abiejų sektorių atstovai.

1.13 Tyrimo organizavimas

Ekspertai buvo supažindinti su keliamos problemos aktualumu. Ekspertams (4 ir 5) klausimai buvo pateikti žodžiu gyvo interviu metu. Ekspertams (1 ir 2) klausimynas buvo išsiųstas el. paštu, o interviu su ekspertu (3) buvo vykdomas telefonu.

1.14 Tyrimo duomenų analizė

Pirmasis klausimas: pažymėtina, kad visi be išimties ekspertai (1-5) kaip didžiausias problemas kibernetinio saugumo srityje įžvelgia finansavimo trūkumą, bendro supratimo apie kibernetines grėsmes suvokimo nebuvimą bei ypatingos svarbos informacinės infrastruktūros sąrašo nebuvimą. Ekspertas 4 ypatingą dėmesį akcentavo į piktavališkus kitų valstybių neteisėtus veiksmus kibernetinėje erdvėje ir būtinybę į tai atkreipti dėmesį. Pasak eksperto, valstybės turi neribotus tiek žmogiškuosius, tiek ir finansinius išteklius organizuoti kibernetines atakas.

Kol nebus identifikuotos ypatingos svarbos informacinės infrastruktūros, tol Nacionalinis kibernetinio saugumo centras negalės sklandžiai ir užtikrintai vykdyti savo pareigų susijusių su kibernetinių incidentų tyrimais ir prevencija. Tiek privačios įmonės, tiek ir viešasis sektorius per mažai investuoja į saugumo prevenciją, jaučiamas mokymų ir švietimo trūkumas elektroninės informacijos saugos srityje, o taip elektroninės informacijos saugos specialistų trūkumas.

Antrasis klausimas: pasak ekspertų (1-5), saugumo trūkumas jaučiamas tiek viešajame, tiek ir privačiame sektoriuje, taigi vieningos nuomonės, kuris sektorius nuo kibernetinių grėsmių apsisaugojęs geriau nėra. Pasak ekspertų (1-2), privatus sektorius iš dalies yra saugesnis, nes yra labiau suinteresuotas saugoti savo informaciją ir reputaciją, nes nuo to tiesiogiai priklauso įmonės pelnas, o taip pat privatusis sektorius turi didesnes finansines galimybes pasisamdyti geresnius saugumo specialistus.

Trečias klausimas: apie tai, kad dabartinė (po LR Kibernetinio saugumo įstatymo priėmimo) Lietuvos teisinė bazė yra pakankama norint užtikrinti aiškų institucinį atsakomybių paskirstymą, pasisakė (1,2,3) ekspertai, tačiau jie pabrėžė, kad trūksta operatyvaus bendradarbiavimo tarp institucijų. Eksperto 3,4,5 nuomone būtina atnaujinti Kibernetinio saugumo plėtros programą 2011-2019 metams, kuriame turi būti atsižvelgta į tai, kad už kibernetinio saugumo politikos formavimą ir organizavimą dabar yra atsakinga nebe Vidaus reikalų ministerija, o Krašto apsaugos ministerija.

Ketvirtasis klausimas: kalbant apie Lietuvos Respublikos Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 programoje buvo iškeltą strateginis tikslas – „plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus 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 Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis pasiektų 60 procentų“, eksperto 1, 3 ir 5 nuomone, Lietuva plėtodama šį tikslą eina sėkminga linkme, bet kiek per lėtai. Taip pat, eksperto 3 manymu, reiktų pakoreguoti plėtros programoje nustatytus tikslus atsižvelgiant į dabartinę Lietuvos situaciją. Ekspertas 5 pabrėžė, kad Lietuva sugebėtų gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalį padidinti ir iki daugiau nei 60 procentų, jei kalba eitų apie kokybiško interneto ryšio užtikrinimą, tačiau ne apie elektroninių nusikaltimų suvaldymą. Pasak eksperto 2, kol nebus išspręstos problemos susijusios su komunikacija, tol šis tikslas pilnai nebus pasiektas. Kibernetiniai incidentai yra įvairaus pobūdžio ir sunkesnių incidentų sprendimas gali užtrukti nemažai laiko.

Penktasis klausimas: visi ekspertai pritarė, kad būtina kuo skubiau identifikuoti ypatingos svarbos informacinių infrastruktūrų objektus. Tam visų pirma Vidaus reikalų ministerija turi parengti metodiką, pagal kurioje esančius kriterijus Nacionalinis kibernetinio saugumo centras identifikuos ypatingos svarbos informacinių infrastruktūrų objektus. Kol kas sąrašas yra tik „numanomas“. Į jį patenka tie sektoriai, dėl kurių netekimo, kiltų nacionalinio saugumo problema, pasak eksperto 1 tai yra šie sektoriai: vandens, elektros tiekimo, ryšio tiekimo, bankai ir pan. Pasak eksperto 5, ypatingos svarbos infrastruktūra yra šie sektoriai: energetika, transportas, vandens paslaugos, bankininkystė, finansų rinkų infrastruktūra, sveikatos sektorius, maisto tiekimo grandinė, interneto mainų mazgai, IRT: debesijos kompiuterijos paslaugos, kurias operatorius naudoja bet kurioms prieš tai išvardintoms paslaugoms teikti.

Šeštasis klausimas: pažymėtina, kad visi be išimties ekspertai (1-5) įvardijo į ką kreiptis Lietuvos piliečiui, kuris patyrė kibernetinį incidentą. Viskas priklauso nuo incidento pobūdžio. Visų pirma iškilus interneto ryšio problemai reiktų kreiptis į ryšio tiekėją, o jei įtariama kriminalinė veika, tuomet būtina kreiptis į policiją. Ekspertas 1 akcentavo, kad visų pirma kiekvienas pilietis turi atsakingai vertinti grėsmes kylančias internete ir stengtis kaip įmanoma patiems nuo jų apsisaugoti. Eksperto 2 nuomone, Kibernetinio saugumo centras taip pat neturėtų atsisakyti pakonsultuoti pilietį ir jį nukreipti tinkama linkme.

Septintasis klausimas: ruošiant Lietuvos Respublikos Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 programą ir Kibernetinio saugumo įstatymą, ekspertų nuomone, atsižvelgiant į Lietuvos situaciją buvo remiamasi kitų šalių gerosiomis

praktikomis: Suomijos, Švedijos, Izraelio, Estijos, Latvijos, Čekijos, Vokietijos, Didžiosios Britanijos (tiek strategijomis, tiek ir įstatymais).

Aštuntasis klausimas: ekspertai vienbalsiai Lietuvos situaciją ES ir NATO kontekste vertina palankiai. Nesame lyderiai, tačiau tikrai ir ne paskutiniai. Eksperto 2 nuomone, gaila, kad Kibernetinio saugumo įstatymas priimtas tik 2014 metais, todėl žengiame tik pirmuosius žingsnius kibernetinio saugumo užtikrinimo link. Eksperto 3 nuomone, Lietuva padarė pažangą teisinėje srityje, tačiau negalima „užmigti ant laurų“, nes kibernetinio saugumo sritis yra labai dinamiška. Ekspertas 4 pabrėžė Lietuvos bendradarbiavimo su užsienio šalimis ir organizacijomis svarbą.

Devintasis klausimas: kalbant apie Lietuvos kibernetinio saugumo strategijos kūrimą, ekspertų nuomonės išsiskyrė. Vieni teigė, kad naujos strategijos nereikia, kiti teigė, kad reikia. Galima priimti išvadą, kad būtinas bent jau esamos plėtros programos pakeitimas ir patobulinimas atsižvelgiant į pakitusią Lietuvos situaciją ir Kibernetinio saugumo įstatymo nuostatus.

Dešimtasis klausimas: ekspertai (2-5) sutiko, kad kibernetinio saugumo pratybos yra vienas efektyviausių metodų, kuris padeda įvertinti pasirengimo būklę kibernetinio incidento atveju. Kibernetinio saugumo pratybos vyksta tiek nacionaliniu, tiek ir tarptautiniu mastu. Pratybos leidžia įsivertinti institucijoms, kur yra jų silpniausios vietos ir tai tobulinti, siekiant išvengti tikrų incidentų. Ekspertas 2 teigė, jog CERT- LT vykdomų pratybų metu paaiškėjo, kad susiduriama su sunkumais viešojo ir privataus sektoriaus komunikacijos srityje. Ekspertas 2 pabrėžė problemą, kad itin trūkta „konkrečiai už kibernetinio saugumo situacijos organizavimą atsakingų asmenų bei apibrėžtumo, kas už ką atsakingas, į ką reikia kreiptis ir kokiomis priemonėmis kreiptis“. Taigi, būtina atkreipti dėmesį į su komunikacija susijusią problemą ir ją spręsti.

Apibendrinant**,** kibernetinio saugumo užtikrinimas yra sudėtingas uždavinys valstybei. Šioje srityje susiduria politiniai, finansiniai bei visuomeniniai elementai, kurie yra lemiami tiek aukščiausių valstybės institucijų (formuojant politiką), tiek atskirų privataus sektoriaus įmonių (koordinuojant savo veiksmus) tiek ir pavienių šalies piliečių. Sėkmingą kibernetinio saugumo valdymą lemia efektyvus veiksmų vykdymas ir šalies, ir bendradarbiaujant su užsienio partneriais.

Strategijos turėjimas dar neužtikrina kibernetinio saugumo šalyje. Būtinas sklandus jos vykdymas – apibrėžtas politikos vykdymas, tikslingas institucijų funkcijų organizavimas, bendradarbiavimo užtikrinimas nacionaliniu ir tarptautiniu mastu bei tikslingas išteklių paskirstymas, ypatingos svarbos infrastruktūrų identifikavimas.

Formuojant strategiją ir politiką *ypatingos svarbos infrastruktūrų identifikavimas yra prioritetinis veiksmas.* Tuomet seka grėsmių bei priemonių su jomis susidoroti identifikavimas. Tik atsakius į klausimus: *ką ginti, nuo ko ginti ir kokiomis priemonėmis ginti*, galima užtikrinti sklandų kibernetinio saugumo užtikrinimo veiksmų planą.

Vienas iš svarbiausių aspektų kalbant apie kibernetinę saugumo užtikrinimą yra klausimas, ką reikia ginti. Šiuo atžvilgiu tiek atskiros valstybės, tiek valstybių sąjungos (pvz.: Europos Sąjunga) turi ypatingos svarbos infrastruktūrą, kuri yra ginama įvykus kibernetiniam incidentui. Europos Sąjunga yra identifikavusi ypatingos svarbos infrastruktūrą iš 2 pagrindinių (energetika; transportas) sektorių ir 11 subsektorių. Siekiant apsaugoti šią infrastruktūrą Europos Taryba yra paruošusi direktyvą dėl „Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo“. Taip pat, savo ypatingos svarbos infrastruktūrą identifikavo ir NATO, kuri yra sudaryta iš 3 pagrindinių sektorių ir 10 subsektorių.

Remiantis Lietuvos teisės aktais, svarbią strateginę reikšmę nacionaliniam saugumui turi šie ūkio sektoriai:

1) energetikos;

2) transporto;

3) informacinių technologijų ir telekomunikacijų, kitų aukštųjų technologijų;

4) finansų ir kredito. (Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymo Nr. IX-1132 1, 2, 3 ir 7 straipsnių pakeitimo įstatymas, 2014).

Kai kurios analizuotos darbe valstybės savo ypatingos svarbos infrastruktūrą išskyrė ir prioretizavo savaip. Vokietija išskyrė tokius sektorius: transportas ir eismas; energetika; pavojingos medžiagos; telekomunikacijos ir informacinės technologijos; finansai ir draudimas; paslaugos (sveikatos, vandens ir pan.); viešas administravimas ir teisinė sistema; kiti (kultūros paveldas ir pan.). JAV išskirdama ypatingos svarbos infrastruktūrą identifikavo šias sritis: finansines paslaugas; transportavimą; viešus darbus (energijos bei vandens tiekimą, gelbėjimo tarnybos ir pan.); kosmosą; logistiką; pasiruošimas krizinėms situacijoms; sveikatos apsauga; personalas; gynybos informacinė infrastruktūra; valdymas, kontrolė ir ryšiai; žvalgyba ir žvalgymas. Šie išvardinti ypatingos svarbos infrastruktūros sektoriai sudaryti iš smulkesnių informacinės infrastruktūros objektų. Būtina paminėti, kad Austrija savo oficialaus ypatingos svarbos infrastruktūrų sąrašo neturi.

Pagal LR kibernetinio saugumo įstatymą, už ypatingos svarbos informacinės infrastruktūros saugumą yra atsakingas Nacionalinis kibernetinio saugumo centras, tačiau Lietuvoje ypatingos svarbos informacinė infrastruktūra šiuo metu nėra identifikuota. Remiantis Lietuvos ekspertų užsienio valstybių patirtimi, ypatingos svarbos infrastruktūromis reiktų laikyti:

- energetikos sektorių;
- finansines ir draudimo institucijas;
- telekomunikacijų operatorius;
- interneto paslaugų tiekėjus;
- sveikatos apsaugos institucijas;

- transporto sektorių;
- oro transportą;
- karines struktūras ir priemones;
- Valstybines paslaugas;
- vandentiekio ir nuotekų šalinimo sistemas;
- maisto gamybos segmentas;
- pagrindiniai internetiniai portalai bei televizija.

Taip pat, būtina atlikti pataisas Kibernetinio saugumo plėtros 2011-2019 metais programoje, nes kaip teigia LR kibernetinio saugumo įstatymas, visos kibernetinio saugumo politikos koordinavimo pareigos, kurios prieš tai teko *Vidaus reikalų ministerijai*, dabar yra perduotos *LR krašto apsaugos ministerijai*, taigi, turime problemą, kadangi šiai dienai du teisiniai dokumentai prieštarauja vienas kitam.

Pagal LR kibernetinio saugumo įstatymą, tiek NKSC tiek ir elektroninių viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų bei elektroninės informacijos prieglobos paslaugų tiekėjai privalo teikti paslaugų gavėjams rekomendacijas apie priemones kibernetiniam saugumui užtikrinti naudojantis teikiamomis paslaugomis. Tačiau, kol nebus suformuota „kibernetinio saugumo kultūra“ ir vartotojai patys nesupras rizikos, su kuria susiduria, šios rekomendacijos gali būti bevertės.

Pasak tyrime dalyvavusių ekspertų, kibernetinio saugumo pratybos yra vienas efektyviausių metodų, kuris padeda įvertinti pasirengimo būklę kibernetinio incidento atveju. Lietuvos Respublikos ryšių reguliavimo tarnyba vykdo kibernetinio saugumo pratybas, kuriose dalyvauja 25 valstybinės institucijos, 8 bankų atstovai ir 10 Lietuvos ir užsienio valstybių CERT padaliniai. Pratybos vyksta specialiai joms sukurtoje platformoje, kuri leidžia valdyti galimų kibernetinių atakų scenarijų užduotis ir stebėti kiekvieno etapo vykdymą.

Pratybų tikslas – stiprinti tarpinstitucinį bendradarbiavimą sprendžiant kibernetinius incidentus, komunikacijos spartą, būtinybę kritinėse situacijose rasti atsakingų institucijų atstovų kontaktus, pasirengimą naudoti lengvai prieinamas šifravimo priemones duomenų perdavimui viešaisiais tinklais ir lavinti įgūdžius operatyviai keistis informacija galimų kibernetinių incidentų metu.

Pratybos leidžia įsivertinti institucijoms, kur yra jų silpniausios vietos ir tai tobulinti, siekiant išvengti tikrų incidentų. Šis metodas padėtų įsitikinti, ar tinkamai veikia saugumo sistemos ir būtų lengviau pastebėti kurias sritis būtina stiprinti.

IŠVADOS

1. Apibendrinant visas analizuotas strategijas, penkios iš septynių šalių pateikia aiškius kibernetinio saugumo sąvokos apibrėžimus. Tam kad nekiltų nesklandumų bendradarbiaujant tarptautiniu lygiu *būtinas tarptautiniu mastu pripažintas ir suderintas kibernetinio saugumo apibrėžimas.*
2. Dauguma strategijų pripažįsta, visuomenės informuotumo poreikį ir piliečių požiūrio formavimą į kibernetinį saugumą, tačiau kaip strateginį tikslą „kibernetinio saugumo kultūros“ formavimą ir piliečių atsakomybės stiprinimą išskiria tik Austrija. Atlikto ekspertinio interviu rezultatai parodė, kad Lietuva taip pat susiduria su kibernetinių grėsmių suvokimo problema.

   Atsižvelgiant į vyraujančias tendencijas būtina apibrėžti užsienio valstybių priešiškus veiksmus kibernetinėje erdvėje kaip vieną didžiausių grėsmių, kadangi būtent valstybės turi didžiausius kibernetinius pajėgumus, nukreiptus rinkti informaciją, trikdyti automatizuoto duomenų apdorojimo sistemų ir tinklų funkcionavimą, juos užvaldyti arba kitaip paveikti ir taip pakenkti nacionaliniam saugumui.

   Vokietijos, Kanados ir Naujosios Zelandijos strategijoje pasakyta, kad kibernetinių incidentų pavojus gresia tik toms sistemoms, kurios yra prijungtos prie pasaulinio tinklo. Tačiau prisiminus *Stuxnet* atvejį, toks šalių požiūris gali būti laikomas atsainiu. Kibernetinę ataką galima įvykdyti ir tose sistemose, kurios nėra prijungtos prie išorinio tinklo, yra būdų, kaip kenksmingą kodą galima paskleisti nesinaudojant internetu.

   Kadangi, kibernetinė erdvė yra visuotinė, svarbus šalių bendradarbiavimas tarptautiniu lygmeniu. Europos Sąjungos valstybės teigia, kad reikalingas glaudesnis Europos Sąjungos šalių narių bendradarbiavimas siekiant pažaboti kibernetinius nusikaltimais. *Apibendrinant analizuotų valstybių kibernetinio saugumo strategijas, pastebima, kad visos valstybės kelia panašius tikslus, susijusius su tarpusavio bendradarbiavimu tiek nacionaliniu, tiek tarptautiniu lygiu*.

   Didelį kibernetinių incidentų skaičių šalyse gali lemti ir *valstybės geopolitinė situacija ir veiksmai*. Politiškai aktyvios ir pasisakančios valstybės gali sulaukti daugiau kibernetinių incidentų nei „ramios“ valstybės. Taip pat, kibernetinių incidentų didelį mastą gali lemti *puikiai išvystyta interneto infrastruktūra*, kuri gali būti kaip jaukas piktavaliams programišiams ir skatinti juos pasinaudoti puikios infrastruktūros teikiamais privalumais atliekant nusikaltimus. Pastebimas *santykis tarp šalies ekonominės situacijos ir kibernetinių incidentų skaičiaus*. Kuo šalis turtingesnė tuo ji potencialiai patrauklesnė kibernetiniams nusikaltėliams.

3. Pagal LR kibernetinio saugumo įstatymą, už ypatingos svarbos informacinės infrastruktūros saugumą yra atsakingas Nacionalinis kibernetinio saugumo centras, tačiau Lietuvoje ypatingos svarbos informacinė infrastruktūra šiuo metu nėra identifikuota. Formuojant saugumo strategiją politiką *ypatingos svarbos infrastruktūrų identifikavimas yra prioritetinis veiksmas.* Tuomet seka grėsmių bei priemonių su jomis susidoroti identifikavimas. Tik atsakius į klausimus: *ką ginti, nuo ko ginti ir kokiomis priemonėmis ginti*, galima užtikrinti sklandų kibernetinio saugumo užtikrinimo veiksmų planą.

   Kibernetinio saugumo plėtros 2011-2019 metais programoje yra neatitikimų dėl kibernetinio saugumo politikos formavimo ir įgyvendinimo (pagal plėtros programą šią pareigą vykdo *LR Vidaus reikalų ministerija*), tačiau, pagal LR kibernetinio saugumo įstatymą funkcijos yra perduotos *LR krašto apsaugos ministerijai*.
4. Pasak tyrime dalyvavusių ekspertų, kibernetinio saugumo pratybos (angl. *penetration test*) yra vienas efektyviausių metodų, kuris padeda įvertinti pasirengimo būklę kibernetinio incidento atveju. Pratybos vyksta specialiai joms sukurtoje platformoje, kuri leidžia valdyti galimų kibernetinių atakų scenarijų užduotis ir stebėti kiekvieno etapo vykdymą.

   Prognozuojama, kad kibernetinių incidentų skaičius bent jau artimiausiu metu nemažės, kibernetinė erdvė išliks viena pagrindinių veiklos erdvių vykdant neteisėtus veiksmus, ar kitaip veikiant svarbius Lietuvos nacionaliniam saugumui objektus.

PASIŪLYMAI

1. Siūlytina priimti *tarptautiniu mastu pripažintą ir suderintą kibernetinio saugumo apibrėžimą.*
2. Siekiant užtikrinti Lietuvos gyventojų saugumą kibernetinėje erdvėje siūlytina ugdyti supratimą apie kibernetinėje erdvėje tykančius pavojus ir formuoti *„kibernetinio saugumo kultūrą“*. Tam reikalingas švietimas kibernetinio srityje, kuris galėtų būti ugdomas mokyklose, darbo vietose. Pagal dabartinę statistiką, valstybinių institucijų darbuotojų švietimas kompiuterinių technologijų srityje, o taip pat ir kompiuterio saugumo srityje yra menkas. Privatusis sektorius taip pat nelinkęs daug investuoti nei į darbuotojų apmokymus, nei į elektronines duomenų apsaugos programas.
3. Tam, kad kibernetiniai nusikaltimai būtų suvaldomi visuotiniu (tarptautiniu) lygiu siūlytina priimti bendrą valstybių požiūrį į kibernetinį saugumą. ES narėms siūlytina stengtis suvienodinti savo strateginius tikslus, principus, prioritetus ir veiklos sritis, tam, kad būtų formuojamas vieningas suvokimas ir taip būtų lengviau siekti bendro tikslo. ES šalys atsižvelgdamos į 2013 metais išleistą ES kibernetinio saugumo strategiją galėtų ją panaudoti kaip gaires formuojant savo nacionalines kibernetinio saugumo strategijas.
4. Lietuvoje siūlytina kuo greičiau identifikuoti ypatingos svarbos informacinės infrastruktūros objektus. Siūlytina į ypatingos svarbos informacinės infrastruktūros objektų sąrašą įtraukti šiuos sektorius: *energetikos sektorių; finansines ir draudimo institucijas; telekomunikacijų operatorius; interneto paslaugų tiekėjus; sveikatos apsaugos institucijas; transporto sektorių; oro transportą; karines struktūras ir priemones; valstybines paslaugas; vandentiekio ir nuotekų šalinimo sistemas; maisto gamybos segmentas; pagrindiniai internetiniai portalai bei televizija.*
5. Siūlytina atlikti pataisas Kibernetinio saugumo plėtros 2011-2019 metais programoje ir perduoti kibernetinio saugumo politikos koordinavimo ir vykdymo pareigas *LR krašto apsaugos ministerijai*.
6. Vienas efektyviausių metodų siekiant užtikrinti kibernetinį saugumą yra pratybų vykdymas (angl. *penetration test*). Siūlytina vykdyti pratybas įtraukiant ne tik valstybines ir finansines institucijas ir, bet ir kuo daugiau privačiojo sektoriaus įmonių. Taip pat, siūlytina, kad pratybose dalyvautų visi sektoriai, kurie bus įtraukti į *ypatingos svarbos informacinės infrastruktūros objektų sąrašą*. Pratybų vykdymas įtraukiant į jas kritinius objektus yra svarbus nacionaliniam saugumui užtikrinti. Kibernetinę ataką galima įvykdyti ir tose sistemose, kurios nėra prijungtos prie išorinio tinklo, yra būdų, kaip kenksmingą kodą galima paskleisti nesinaudojant internetu. Todėl siūlytina užtikrinti priemones, kuriomis būtų galima patikrinti ypatingos svarbos objektų pasirengimą atremti kibernetines atakas „iš vidaus“, t. y., kai sistemos nėra prijungtos prie tinklo. Siūlytina kibernetinio saugumo srityje stiprinti

finansavimą siekiant apsaugoti valstybinės svarbos sistemas ir informacinius tinklus siekiant sumažinti pažeidžiamumo lygį plėtojant kibernetinę gynybą vykdant aktyvią prevenciją.

LITERATŪRA

1. 2014 metų veiklos apibendrinimas. *CERT-LT*. Prieiga per internetą: <https://www.cert.lt/pranesimai/cert-lt_apibendrina_2014_metu_veikla_7cc.html>.
2. 2015-ieji – atakų prieš bankus ir verslą metai (2014-12-29). *Technologijos.lt*. Prieiga per internetą: <*http://it.lrytas.lt/ismanyk/2015-ieji-ataku-pries-bankus-ir-versla-metai.htm>.*
3. A Secure Europe in a Better World, European Security Strategy. Brussels, 12 December 2003. Prieiga per internetą: <*http://www.consilium.europa.eu/uedocs/cmsupload/78367.pdf*>.
4. Action Plan for Critical Infrastructure 2014-2017. Canada. *Cooperative Cyber Defense Centre of Excellence: Cyber Security Strategy Documents*. Prieiga per internetą: <*http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf* >.
5. Amount of monetary damage caused by reported cybercrime to the IC3 from 2001 to 2014 (in million U.S. dollars). (2014). *Statista*. Prieiga per internetą: <*http://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/>.*
6. Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos. (2014). *Grėsmių nacionaliniam saugumui vertinimas*. Vilnius. Prieiga per internetą: *http://www.kam.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/aotd.html*.
7. Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos. (2015). *Grėsmių nacionaliniam saugumui vertinimas*. Vilnius. Prieiga per internetą: *http://www.kam.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/aotd.html*.
8. Atkočiūnienė, Z., O. (2006). Informacijų ir žinių vadyba informacijos ir komunikacijos mokslų sistemoje. *Informacijos mokslai*. Prieiga per internetą: *http://etalpykla.lituanistikadb.lt/fedora/objects/LT-LDB-0001:J.04~2006~1367153950676/datastreams/DS.002.0.01.ARTIC/content.*
9. Augustinaitis A., Rudzkienė V., Petrauskas, R. A., Dagytė, I., Martinaitytė, E., Leichteris, E., Malinauskienė, E., Višnevska, V., Žilionienė, I. (2009). Kolektyvinė monografija. *Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas*. Vilnius. Mykolo Romerio universiteto Leidybos centras, 352 p.
10. Austrian Security Strategy. Security in a new decade – Shaping Security. (2013). Viena. *Cooperative Cyber Defense Centre of Excellence: Cyber Security Strategy Documents*. Prieiga per internetą: <*https://www.bka.gv.at/DocView.axd?CobId=52251*>.
11. Austrian Cyber Security Strategy. (2013). Viena. *Cooperative Cyber Defense Centre of Excellence: Cyber Security Strategy Documents.* Prieiga per internetą: <https://www.bka.gv.at/DocView.axd?CobId=50999>.

12. BENDRAS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI Europos Sąjungos kibernetinio saugumo strategija: atvira, saugi ir patikima kibernetinė erdvė. 2013 m. vasario 7 d., Briuselis. Prieiga per internetą: <*http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52013JC0001*>.
13. Botnet tinklai. *E saugumas*. Prieiga per internetą: <http://www.esaugumas.lt/lt/botnetai.html>.
14. Brock, W. A., Hommes, C. H. (1997). A rational route to randomness. *Econometrica*. Vol. 65, Nr. 5, 1059-1095.
15. Canada First Defense Strategy. (2010). Canada. *Cooperative Cyber Defense Centre of Excellence: Cyber Security Strategy Documents*. Prieiga per internetą: <*http://www.forces.gc.ca/assets/FORCES_Internet/docs/en/about/CFDS-SDCD-eng.pdf* >.
16. Center for Strategic and International Studies & McAfee. (2013). *The economic impact of cybercrime and cyber espionage*. Prieiga per internetą: <*http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime.pdf?view=legacy*>.
17. Center for Strategic and International Studies & McAfee. (2014). *Net Losses Estimating the Global Cost of Cybercrim*e. Prieiga per internetą: <*http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf?view=legacy*>.
18. CYBER SECURITY STRATEGY OF THE CZECH REPUBLIC FOR THE 2011 – 2015 PERIOD. (2011). Prieiga per internetą: <*https://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF>.*
19. Daugelio kibernetinių grėsmių sukėlėjai – patys valdininkai (2014-11-17). *Lrytas.lt.* Prieiga per internetą: <*http://it.lrytas.lt/ismanyk/daugelio-kibernetiniu-gresmiu-sukelejai-patys-valdininkai.htm>.*
20. Defense Policy Guidelines. (2011). *NATO Cooperative Cyber Defense Centre of Excellence: Cyber Security Strategy Documents*. Prieiga per internetą: <*http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=157024*>.
21. Elektroninis saugumas: grėsmių išvengimo planai Europoje (2015.03.16). *Europos Parlamentas*. Prieiga per internetą: <*http://www.europarltv.europa.eu/lt/player.aspx?pid=9538deaf-31a4-4910-9c2f-a45a00ea068e*>.

22. French White Paper. Defense and National security. (2013). France. *Cooperative Cyber Defense Centre of Excellence: Cyber Security Strategy Documents*. Prieiga per internetą: <*https://ccdcoe.org/cyber-security-strategy-documents.html*>.
23. Girnienė, I. (2010). Informacijos vadyba šiuolaikinėje organizacijoje. Prieiga per internetą: <*https://www.esec.vu.lt/straipsniai/index.php/elearning/article/download/12/12 failo*>.
24. Halder, D., Jaishankar, K. (2011). *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, USA.
25. Harašta, J., (2013). Cyber Security in Young Democracies. *Jurisprudencija*. 20(4), p.1457-1472. Prieiga per internetą: *https://www3.mruni.eu/ojs/jurisprudence/article/view/1854/1696.*
26. Information systems defense and security, France ‘s strategy. (2011). *Cooperative Cyber Defense Centre of Excellence: Cyber Security Strategy Documents*. Prieiga per internetą: <*http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf*>.
27. Japertas S. (2010). Kibernetinėms atakoms Lietuva nepasiruošusi. *Technologijos.lt*. Prieiga per internetą: <*http://m.technologijos.lt/cat/1/article/S-16509*>.
28. Japertas, S. (2010-03-23). KIBERNETINĖ SAUGA IR LIETUVA. *Bernardinai.lt*. Prieiga per internetą: <*http://www.bernardinai.lt/straipsnis/2010-03-23-saulius-japertas-kibernetine-sauga-ir-lietuva/42433*>.
29. Justiuginas, S. (2011). Informacijos saugumo valdymas Lietuvos viešajame sektoriuje. *Informacijos mokslai*. p. 7-25. Prieiga per internetą: *www.zurnalai.vu.lt/informacijos-mokslai/article/download/3137/2261.*
30. Karspersky Lab report. (2015). *Spam & Phishing in Q1 2015*. Prieiga per internetą: <*https://securelist.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015/*>.
31. Karspersky Lab. (2015). *Spam & Phishing in Q2 2015*. Prieiga per internetą: <https://securelist.com/files/2015/08/KL_Q2_2015_SPAM_REPORT_ENG.pdf>
32. Kelley, M. (2013-11-20). The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. *BusinessInsider.com.* Prieiga per internetą: <*http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11*>.
33. Kiškis, M., Petrauskas, R., Rotomskis I., Štitilis, D. (2006). *Teisės informatika ir informatikos teisė*. Mykolo Romerio universitetas, Vilnius.
34. Kompiuterinis „kirminas“ paralyžiavo ligoninės darbą (2011-12-27). *Technologijos.lt*. Prieiga per internetą: <*http://www.technologijos.lt/n/technologijos/it/S-23491/straipsnis/Kompiuterinis-kirminas-paralyziavo-ligonines-darba*>.

35. Konvencija dėl elektroninių nusikaltimų. 2001 m. Lapkričio 23 d. *Teisės aktų registras*. Prieiga per internetą: <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=228195&p_query=&p_tr2=>.
36. KTU ekspertas: Lietuva – kibernetinio karo apkasuose (2014-09-25). *Technologijos.lt* Prieiga per internetą: <*http://www.technologijos.lt/n/technologijos/it/S-42947/straipsnis/KTU-ekspertas-Lietuva--kibernetinio-karo-apkasuose>.*
37. Lietuvoje plinta pavojingas virusas: saugokite savo duomenis (2015-08-28). *Technologijos.lt*. Prieiga per internetą: <*http://www.technologijos.lt/n/technologijos/it/S-49840/straipsnis/Lietuvoje-plinta-pavojingas-virusas-saugokite-savo duomenis?utm_source=Susije_po_straipsniu&utm_medium=Vidine_navigacija&utm_campaign=Vidine_navigacija*>.
38. Lietuvos Respublikos kibernetinio saugumo įstatymas. 2014 m. Gruodžio 11 d. Nr. XII-1428. *Teisės aktų registras*. Prieiga per internetą: <*https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4*>.
39. Lietuvos Respublikos nutarimas, Dėl nacionalinio saugumo strategijos patvirtinimo, 2002 m. gegužės 28 d. Prieiga per internetą: <*http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=429234>*
40. Lietuvos Respublikos ryšių reguliavimo tarnyba. *Tinklų ir informacijos saugumas*. Prieiga per internetą: <*http://www.rrt.lt/lt/vartotojui/tinklu-informacijos-saugumas-vartotojui.html*>.
41. Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymo Nr. IX-1132 1, 2, 3 ir 7 straipsnių pakeitimo įstatymas. 2014. *Teisės aktų registras*. Prieiga per internetą: *https://www.e-tar.lt/portal/lt/legalAct/332e48b059ed11e487eff7b424bd0f08.*
42. Lietuvos Respublikos vyriausybės 2011 metų birželio 29 dienos nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“. *Teisės aktų registras*. Vilnius. Prieiga per internetą: *https://www.e-tar.lt/portal/lt/legalAct/TAR.1ABB945646B7*.
43. Luiijf, H. A. M., Besseling, K., Spoelstra M., de Graaf, P. (2013). *Ten National Cyber Security Strategies: A Comparison.* CRITIS 2011, LNCS 6983, p.1-17. Springer- Verland Berlin Heidelberg.
44. Mankevičius, V. LMA TECHNIKOS MOKSLŲ SKYRIUS SURENGĖ DISKUSIJĄ „KIBERNETINIS SAUGUMAS“. *Mokslasirtechnika.lt.* Prieiga per internetą: <*http://www.mokslasirtechnika.lt/mokslo-naujienos/lma-technikos-moksl-skyrius-sureng-diskusija-kibernetinis-saugumas.html>.*

45. Moore, R. (2005). *Cybercrime: Investigating High-Technology Computer Crime*. Cleveland, Mississippi.
46. National Cyber Security Strategies. (2012). *Enisa*. Prieiga per internetą: <*https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper*>.
47. National Security Strategy. (2015). *Cooperative Cyber Defense Centre of Excellence: Cyber Security Strategy Documents*. USA. Prieiga per internetą: <*https://ccdcoe.org/sites/default/files/strategy/USA_NSS2015.pdf*>
48. New Zealand ‘s National Security System. (2011). *Cooperative Cyber Defense Centre of Excellence: Cyber Security Strategy Documents*. Prieiga per internetą: <*http://www.dpmc.govt.nz/sites/all/files/publications/national-security-system.pdf*>.
49. NEW ZEALAND’S CYBER SECURITY STRATEGY. (2011). *Cooperative Cyber Defense Centre of Excellence: Cyber Security Strategy Documents*. Prieiga per internetą: <*http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf*>.
50. Nugaraitė, A. (2013). Informacinės erdvės svarba ir valdymas viešojoje valstybės komunikacijoje. *Agora. Politinių komunikacijų studijos.* Nr.2, p. 24-31. Prieiga per internetą: *http://ejournals.vdu.lt/index.php/agora/article/view/502/432.*
51. Parker, D., B. (1989). Computer Crime Criminal Justice Resource Manual, Department of Justice, National Institute of Justice. USA. Prieiga per internetą: *https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf*.
52. PS3 ir iPhone nulaužęs programišius tapo „Google“ saugumo ekspertu (2014-07-22). *Elektronika.lt*. Prieiga per internetą: <*http://www.elektronika.lt/naujienos/ivykiai/45805/ps3-ir-iphone-nulauzes-programisius-tapo-google-saugumo-ekspertu/*>.
53. Report on the Implementation of the European Security Strategy, *Providing Security in a Changing World*, Brussels, 11 December 2008. Prieiga per internetą: <*http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf*>
54. Sapetkaitė, V. (2012 07 23). Kibernetinis (ne)saugumas: Baltijos šalių situacija. *Geopolitika*. Prieiga per internetą: <*http://www.geopolitika.lt/?artc=5504*>.
55. Security Strategy of the Czech Republic. (2015). *Cooperative Cyber Defense Centre of Excellence: Cyber Security Strategy Documents*. Prieiga per internetą: <*http://www.army.cz/images/id_8001_9000/8503/15_02_Security_Strategy_2015.pdf*>.
56. Singh, A., K. (2008). Science & Technology for civil services examinations, *Science & Technology*. P. 198. Prieiga per internetą: *https://goo.gl/Yk4t4A*.
57. Szor, P. (2005). *The art of computer. Virus research and defense.* USA.

58. Štitilis, D. (2013). Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos. *Socialinės technologijos*. 3(1), p. 189–207. Prieiga per internetą: *http://www.mruni.eu/lt/mokslo_darbai/st/paskutinis_numeris/dwn.php?id=351638.*
59. Štitilis, D., Laurinaitis, M. (2009). Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai*. P. 240-247. Prieiga per internetą*:* *http://www.zurnalai.vu.lt/informacijos-mokslai/article/download/3231/2348.*
60. Štitilis, D., Klišauskas, V. (2012). Elektroninės informacijos saugos reglamentavimas Lietuvoje ir Rusijoje: lyginamieji aspektai. *Socialinės technologijos*. 2(2), p. 441–455. Prieiga per internetą: *www.mruni.eu/en/mokslo_darbai/st/archyvas/dwn.php?id=340100.*
61. Štitilis, D., Paškauskas, Ž. (2007). Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. *Socialinės technologijos.* 2(92); p. 37–45. Prieiga per internetą: *https://www.mruni.eu/en/mokslo_darbai/jurisprudencija/archyvas/dwn.php?id=267948.*
62. TARYBOS DIREKTYVA 2008/114/EC, Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo. 2008 m. gruodžio 8 d. *EUR-LEX, Access to European Union law*. Prieiga per internetą*:* *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114*.
63. Tidikis R. (2003). *Socialinių mokslų tyrimų metodologija*. Vilnius. 627 p. Prieiga per internetą: http://www.scribd.com/doc/36462514/Tidikis-Socialiniu-Moksliniu-Tyrimu-Metodologija#scribd.
64. Trylika būdų nužudyti žmogų vien spaudant mygtukus (2015-07-27). *Technologijos.lt*. Prieiga per internetą: <*http://www.technologijos.lt/n/technologijos/it/S-49238/straipsnis/13-budu-nuzudyti-zmogu-vien-spaudant-mygtukus?utm_source=Susije_po_straipsniu&utm_medium=Vidine_navigacija&utm_campaign=Vidine_navigacija>.*
65. Trys ketvirtadaliai interneto naudotojų neatpažįsta grėsmių (2015-10-15). *Lrytas.lt*. Prieiga per internetą: http://it.lrytas.lt/ismanyk/trys-ketvirtadaliai-interneto-naudotoju-neatpazista-gresmiu.htm
66. Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the Word 's First Digital Weapon*. New York.

SANTRAUKA

Informacinių technologijų ir komunikacijų plėtra daro didžiulę įtaką visuomenei pastaraisiais dešimtmečiais. Lemiamos reikšmės tai turi tiek žmogui, kaip atskiram individui, tiek ir visai visuomenei bei verslui. Sparti informacinių technologijų plėtra lėmė tai, kad internetas tapo pagalbine ir neatsiejama priemone. Deja, internetas atnešė ne tik milžinišką naudą. Elektroninės erdvės globalumas suteikė sąlygas vykdyti nusikaltimus iš bet kurios pasaulio vietos ir bet kuriuo paros laiku. Elektroniniai nusikaltimai tapo įprasto nusikalstamumo dalimi. Jie teikia tokias pat neigiamas pasekmės kaip ir tie nusikaltimai, kurie yra atliekami fizinėje erdvėje. Kibernetiniai išpuoliai privertė šalis imtis prevencinių priemonių norint nuo jų apsisaugoti. Siekiant apsaugoti nacionalinę kibernetinę erdvę buvo pradėtos kurti kibernetinio saugumo strategijos ir programos.

Pirmame skyriuje, siekiant išanalizuoti teorinius kibernetinio saugumo valdymo aspektus buvo remiantis mokslinėmis knygomis, moksliniais straipsniai ir interneto medžiaga išanalizuota kibernetinio saugumo svarba Lietuvoje ir pasaulyje. Aptartos kibernetinių nusikaltimų rūšys ir raidos istorija.

Antrame skyriuje buvo analizuota pasaulinė patirtis kibernetinio saugumo srityje, buvo nagrinėtos Kanados, JAV, Prancūzijos, Čekijos, Vokietijos, Austrijos ir Naujosios Zelandijos kibernetinio saugumo strategijos, pateikti pagrindiniai aspektai apie strategijų formavimą ir vykdymą, apibendrinus pateiktos išvados.

Tolesniame skyriuje buvo analizuota kibernetinio saugumo situacija Lietuvoje. Analizuoti LR teisiniai dokumentai reglamentuojantys kibernetinę saugą šalyje: LR Kibernetinio saugumo įstatymas ir LR Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011 – 2019 metais programa.

Išanalizavus dabartinę situaciją Lietuvoje, paskutiniame skyriuje, identifikuotos pagrindinės problemos, buvo pristatytos ekspertams – interviu metodu atlikta ekspertų apklausa. Ekspertų metodu siekta išanalizuoti ir įvertinti Lietuvos kibernetinio saugumo situaciją ir perspektyvas.

SUMMARY

The expansion of information and communication sector had a big influence for people in the recent decades. It not only has an essential meaning for a human itself, but also for the society and business as well. Fast development of information technology made internet a reliable and necessary tool. However, the internet has not only brought positive things. The virtual space has created an opportunity to commit cyber-attacks from anywhere and anytime in the world. Cyber-attacks became a regular part of everyday crime. They have the same consequences as the crimes committed in the physical world. Cyber-attacks have encouraged countries to take action in order to ensure security. To protect national cyber security, safety strategies and programs have been started to be developed. In the first section there was a reliance on scientific books, articles and internet in order to analyze theoretical cyber security management aspects and discuss the importance of cyber security in Lithuania and other world countries. Cyber-crime types and its history were discussed as well.

In the second section global experience of cyber security was analyzed, it included a discussion of Canada's, US, France, Czech Republic's, Germany's, Austria's and New Zealand's cyber security strategies. Main aspects of strategy forming and its carry were concluded. In the further section the situation of Lithuania's cyber security was discussed. Documents regulating cyber security in the country were analyzed, which included Lithuania's cyber security law and electronic safety enlargement program for 2011-2019.

After analyzing current situation in Lithuania, main problems have been identified and presented to the experts in the last section. Interview surveys had been done. Interviews main aim was to analyze and evaluate Lithuania's cyber security situation and its perspective.