MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

Valentinas Mackevičius
Kibernetinio saugumo valdymas

KIBERNETINIO SAUGUMO IŠŠŪKIAI PER KAŠTŲ PRIZMĘ PASAULYJE IR LIETUVOJE

Magistro baigiamasis darbas

Darbo vadovas:
doc. dr. Marius Laurinaitis

VILNIUS, 2021

MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

KIBERNETINIO SAUGUMO IŠŠŪKIAI PER KAŠTŲ PRIZMĘ PASAULYJE IR LIETUVOJE

Kibernetinio saugumo valdymo magistro baigiamasis darbas
Studijų programa *kibernetinio saugumo valdymo* (nuo 2017)

Vadovas:

_____ doc. dr. Marius Laurinaitis

2021-05

Recenzentas

_____

2021-05

Atliko:

_____ KSVvmis 19-1 gr.stud. V. Mackevičius

2021-05

VILNIUS, 2021

TURINYS

PAVEIKSLAI

PRIEDAI

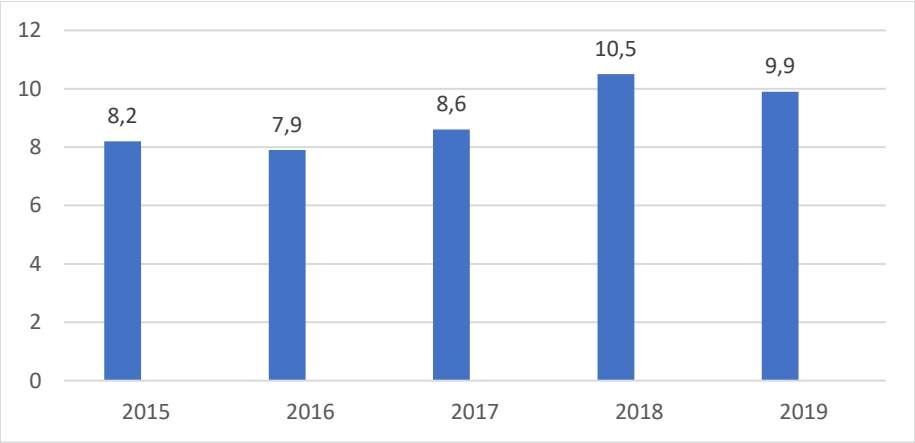
1 priedas. Tyrime panaudotas interviu protokolas

2 priedas. Patvirtinimas apie atlikto darbo savarankiškumą

ĮVADAS

Temos aktualumas ir naujumas. Informacija nuo seno buvo laikoma reikšmingu įrankiu valdžioje, diplomatijoje bei konfliktuose. Nuo 1990 m. informacija vaidina svarbų vaidmenį tarptautiniuose santykiuose bei dėl IKT (informacinių komunikacinių technologijų) tobulėjimo visais gyvenimo aspektais (Cavelty, 2012). Gebėjimas įsisavinti informaciją, jos valdymas, naudojimas, taip pat manipuliavimas informacija tapo aktualiu kariniame lygmenyje, ekonomikoje. Per pastaruosius du dešimtmečius internetas tapo vis svarbesnis šalies ekonominiam konkurencingumui, inovacijų skatinimui ir kiekvieno gyvenimui (Sommestad, 2012). Šiandienos grėsmės kibernetiniam saugumui apima neribotas ir plataus masto atakas. Saugumo trūkumai dažnai baigiasi finansiniais nuostoliais ir nors nepaisant didėjančio supratimo šia tema, pradedant vartotojais ir baigiant dideliais verslais, vis tiek nepasinaudoja turimomis technologijomis ir procesais. Dėl šio bendro investicijų trūkumo įmonėms ir vartotojams kyla didesnė rizika, dėl to ekonominiai nuostoliai patiriami asmeniškai ir bendrai, o tai kelia grėsmę nacionaliniam saugumui (Bodeau, Boyle, Fabius-Greene, Graubart, 2010).

Kibernetinio saugumo tema tampa vis aktualesnė (Heinl, Tan, 2015). Apsaugoti vartotojų, įmonių ir interneto infrastruktūros saugumą niekada nebuvo taip sunku (Seemma, Nandhini, Sowmiya, 2018). Kibernetinių atakų prieš internetinę prekybą (Hartel, Junger, Leijtens, 2015), gyvybiškai svarbius verslo sektorius ir vyriausybines agentūras skaičiai nors ir nėra nuolat augantys, vis dėl to skaičiai išties dideli ir skaičiuojami milijardais. Per pastaruosius penkis metus kenkėjiškų atakų skaičiai:



1 pav. Kenkėjiškų atakų skaičiai 2015-2019 m. milijardais (pagal www.statista.com)

Ši statistika rodo bendrą kenkėjiškų atakų skaičių nuo 2015 iki 2019 m. Paskutiniuoju ataskaitiniu laikotarpiu buvo įvykdyta 9,9 mlrd. kenkėjiškų atakų. Didėjant šioms grėsmėms, saugumo politika, technologijos ir procedūros turi vystytis dar greičiau, norint apsaugoti duomenis, turtą.

Šiandieninėje nuolat besikeičiančioje bei kasdieninį technologinį virsmą patiriančiame pasaulyje įprastos arba kitaip sakant tradicinės grėsmės įkūnija vis naujas formas bei esti vis sunkiau nuspėjamos (Fischer, 2014). Šiuo metu kibernetinio saugumo klausimas pritraukia daug dėmesio tarptautinių konfliktų kontekste. Žiniasklaida bei naujienų portalai reguliariai praneša apie kibernetinį ir informacinį karą. Tai, kad kibernetinis saugumas yra vienas pagrindinių XXI a. iššūkių įrodo 2008 m. įvykęs Rusijos ir Gruzijos konfliktas, kuriame kibernetinė erdvė tapo dviejų šalių konflikto erdve arba 2010 m. kompiuterinis kirminas „Stuxnet“, skirtas pakenkti Irano branduolinei programai, daugelio vertinamas kaip pirmasis geopolitinės reikšmės kibernetinis ginklas, arba Ukrainos krizė, kuri tęsiasi iki šiol (Valuch, 2017). Tai kad kibernetinio saugumo tema netampa mažiau aktuali parodo ir tai, kad teisininkai jau kalba apie galimybes įtraukti civilius gyventojus („kibernetinius šauktinius“) į karines operacijas t.y. sutelkti civilių išteklius karo tikslams bei apie naujas galimybes reaguoti į naujas karo formas: sąmokslų platinimas siekiant demoralizuoti gyventojus ir pan. Kibernetiniame kare dalyvauja ne tik valstybės veikėjai, tačiau ir civiliai gyventojai. Visi pavyzdžiai rodo, kad tradiciniai karo apibrėžimai ir tradiciniai lūkesčiai, kaip atrodo valstybių konfliktai, žlunga XXI a.

Kibernetinio saugumo temos aktualumą įrodo ir NATO, nusprendusi, jog kibernetinė gynyba yra kolektyvinės gynybos dalis. Dėl situacijos rimtumo tarptautinės organizacijos imasi vis naujų atsargumo priemonių priimdamos skirtingos teisinės galios dokumentus, siekiant išspręsti kibernetines grėsmes. Esminė šio darbo tema – kaštų ir kibernetiniam saugumo sąsajos. Remiantis Tarptautinio teisingumo teismo praktika, akivaizdu, kad pagal galiojančias tarptautinės teisės normas karas, kibernetinės atakos, taip pat informaciniai išpuoliai (dažnai įvykdomi taip pat kibernetinėje erdvėje) gali būti suvokiami kaip „karas“ tik tuo atveju, jei vykdomas kartu su fiziniu šalies užpuolimu, kurio dažnai nėra. Daugeliu atvejų kibernetinis karas suvokiamas „tik“ kaip netiesioginis karas, kuris turi būti pasmerktas kaip elgesys, prieštaraujantis tarptautinės teisės principams ir nusikaltimas pagal nacionalinius įstatymus.

Ištirtumas. Kaip jau minėta, kibernetinio saugumo tema tampa vis aktualesnė. Didėjant kibernetinių saugumo pavojui didėja ir kibernetinių saugumo patiriami kaštai (Jang-Jaccard, Nepal, 2014). Vis dėl to trūksta tyrimų, kurie atskleistų koreliacijas tarp kibernetinio saugumo efektyvumą bei kaštus. Lietuvoje vis dar trūksta tyrimų pagrįstu ekspertų vertinimų apie esamas kibernetinio saugumo priemones, kaštus bei jų pačių patirtis. Šiuo tyrimu siekiama nustatyti kaip ekspertai vertiną kibernetinio saugumo temą, ką mano apie skiriamus kaštus bei priemones skirtas kibernetiniam saugumui.

Tyrimo objektas – kibernetinio saugumo kaštų tendencijos.

Tyrimo tikslas – Išanalizuoti kibernetinio saugumo kaštų tendencijas Lietuvoje ir pasaulyje.

Darbo uždaviniai:

1. Atskleisti kibernetinio saugumo sampratą;
2. Išanalizuoti transnacionalinio kibernetinio saugumo padėtį;
3. Atlikti kibernetinio saugumo ekspertų interviu siekiant atskleisti kibernetinio saugumo ir kaštų koreliacijas.

Mokslinė problema. Nacionalinio kibernetinio saugumo centro (NKSC) puslapyje rašoma, jog kibernetinio saugumo prevencija bei pažanga ir kaip tai yra įgyvendinama nacionalinio saugumo bei gynybos labui visuomet prisideda prie kibernetinių incidentų valdymo, kibernetinio saugumo reikalavimų įgyvendinimo stebėsenos ir kontrolės, ypatingos svarbos informacinės infrastruktūros kibernetinio saugumo ir informacinių išteklių akreditacijos. NKSC nuostatuose rašoma, jog pagrindiniai tikslai:

- įgyvendinti nacionalinę kibernetinio saugumo politiką;
- atlikti Saugumo priežiūros tarnybos funkcijas;
- atlikti Nacionalinės komunikacijų apsaugos tarnybos funkcijas;
- vykdyti informacijos sklaidos, tyrimų ir analizės kibernetinio saugumo klausimais veiklą.

Vis dėl to Nacionalinis kibernetinio saugumo centras pripažįsta, jog viena iš aktualiausių kibernetinio saugumo problemų yra pažeidžiamos interneto svetainės, kurios gali būti išnaudotos virusams įdiegti, įsilaužti ar prieigai prie duomenų įgauti, pavyzdžiui, perėmus svetainės administratoriaus paskyrą. Kaip Lietuvoje užtikrinamas kibernetinis saugumas atsižvelgiant į NKSC įvardijamas problemas? Ar skiriamas pakankamas finasavimas kibernetinio saugumo sektoriui? Ar yra nustatytos koreliacijos tarp kaštų ir kibernetinio saugumo?

Ginamieji teiginiai:

1. Kibernetinio saugumo finansavimo trūkumas lemia kibernetines problemas Lietuvoje.
2. Siekiant kibernetinio saugumo efektyvumo svarbu didinti finansavimą.

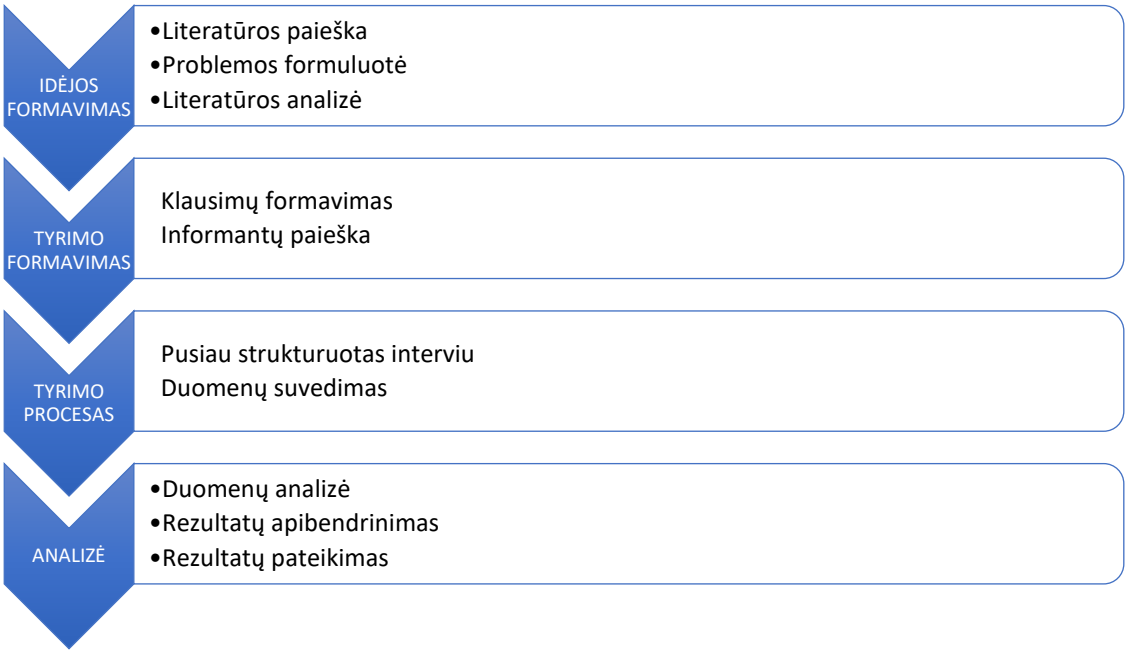
Tyrimo metodika. Tyrimo tikslui pasiekti pasirinkta atlikti kokybinį tyrimą, kuris leistų atskleisti subjektyvią kibernetinio saugumo ekspertų, patirtį, jų nuomonę naudojant socialinius tinklus studijų procese. Kokybinis tyrimo tipas leis atskleisti tyrimo dalyvių požiūrį į tiriamą reiškinį remiantis jų

patirtimis ir suvokimu. Remiantis ekspertų patirtimis, bus mėginama atskleisti, kokios dažniausiai problemos kyla bei su kokiomis problemomis susiduriama.

Pasirinktas duomenų rinkimo instrumentas – pusiau struktūrizuotas individualus interviu, kuris sukuria laisvesnę atmosferą tarp tyrėjo ir tyrimo dalyvio, nes klausimai tik iš dalies standartizuojami, tačiau paliekama erdvė klausti pokalbio eigoje.

Tyrimo laikas: 2020 m. spalio 1-31 d.

Tyrimo etapai:



I - mokslinės literatūros analizė (terminas 2020-03-01 iki 2020-09-01);

II - kokybinio tyrimo instrumento sudarymas (terminas 2020-09-01 iki 2020-09-30);

III - pusiau struktūruotas interviu su kibernetinio saugumo ekspertais (terminas 2020-10-01 iki 2020-10-31);

IV - interviu tekstų turinių analizė (kokybinės turinio (content) analizės metodas, taikant kodavimo procedūras (kategorijų/subkategorijų kūrimą) (terminas 2020-11-01 iki 2020-11-10).

Tyrimo dalyviai: kibernetinio saugumo ekspertai.

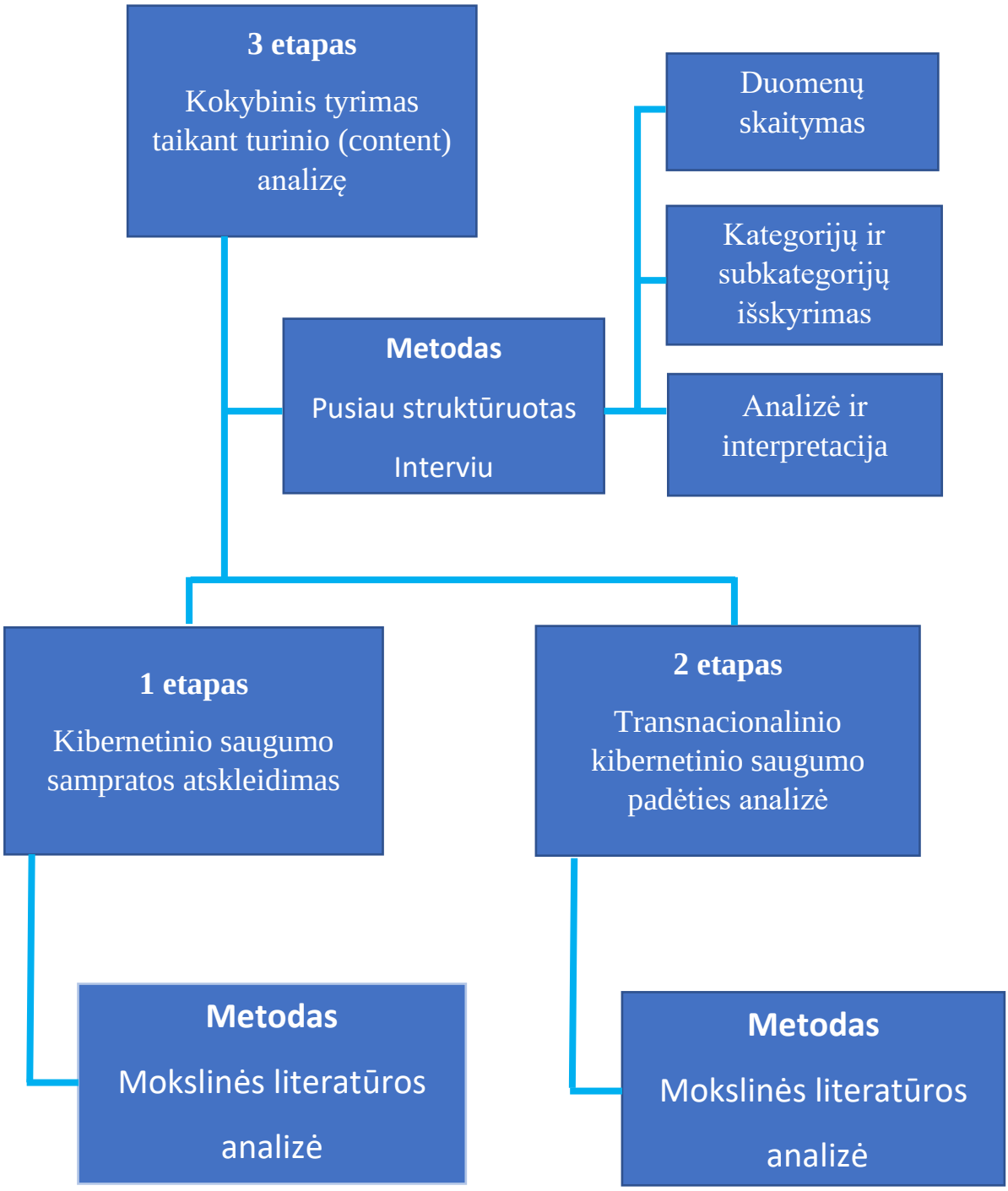
Imties sudarymo būdas. Sudarant tyrimo imtį, bus naudojamas netikimybinės atrankos būdas – tikslinė atranka. Į apklausiamą grupę įtraukiant pačius tipiškiausius bei informatyviausius asmenis tiriamojo požymio atžvilgiu. Todėl šiame tyrime imties tipas bus tikslinė imtis, tai yra kibernetinio saugumo ekspertai.

Tyrimo ribotumas:

- tyrėjo asmeninė patirtis ir žinios gali daryti įtaką pastebėjimams ir išvadoms;

- dėl tyrimo atvirumo tiriamieji gali kontroliuoti duomenų gavimą (surinkimą) ir duomenų rezultatai negali būti patikrinti objektyviai;
- tyrimą gali riboti tyrimą atliekančio nepatyrimas tiek surenkant, tiek analizuojant duomenis.

LOGINĖ SCHEMA



2 pav. Kibernetinio saugumo iššūkiai per kainų prizmę tyrimo loginė schema (sudaryta autoriaus)

1. KIBERNETINIO SAUGUMO SAMPRATA

1.1 Kibernetinio saugumo raida

Internetas yra vienas iš svarbiausių XXI amžiaus išradimų, kurie paveikė mūsų gyvenimą. Šiandien internetas peržengė visas kliūtis ir pakeitė mūsų kalbėjimo, žaidimų, darbo, apsipirkimo, draugų, klausymo, filmų, maisto užsakymo, sąskaitų apmokėjimo, sveikinimo su gimtadieniu / jubiliejumi įpročius ir kt. Internetas palengvino gyvenimą, jis tapo patogesnis. Praėjo tos dienos, kai žmonės turi stovėti ilgoje eilėje norėdami apmokėti telefono ar elektros sąskaitas. Dabar galima sumokėti vienu mygtuko paspaudimu iš savo namų ar darbo. Technologija pasiekė tiek, kad žmonėms net nereikia kompiuterio, norint naudotis internetu. Dabar turint išmanųjį telefoną, planšetinius kompiuterius ir kt., kuriais naudodamiesi internetu žmonės gali palaikyti ryšį su savo draugais, šeima ir darbu visą parą. Internetas supaprastino gyvenimą ir padarė daugelį dalykų lengviau pasiekiamu ir prieinamu (Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts,Wolff, 1997). Dabar internetas leidžia ne tik kalbėtis, bet ir naudotis vaizdo konferencijomis, naudodamas populiarias programas, tokias kaip „Skype“ ir t.t., už labai žemą kainą. Internetas pakeitė ne tik tipinių prietaisų, kuriuos žmonės turi naudojimą. Televizija gali būti naudojama ne tik populiarioms TV laidoms ir filmams žiūrėti, bet ir pokalbiams. Mobilusis telefonas naudojamas ne tik skambinant, bet ir žiūrint naujausią filmą, o buvimo vieta nelemia galimybių. Dirbantys tėvai iš biuro gali stebėti savo vaikus namuose ir padėti jiems atlikti namų darbus, o verslininkas vienu mygtuko paspaudimu gali stebėti savo personalą, biurą, parduotuvę ir kt. Tai palengvino gyvenimo būdą.

Internetas atsirado maždaug 1960 m., kai juo galėjo naudotis tik keli mokslininkai, tyrinėtojai ir gynyba. Iš pradžių kompiuterinis nusikaltimas apsiribojo tik fizine žala kompiuteriui ir su juo susijusia infrastruktūra, tačiau maždaug 1980 m. tendencija pasikeitė - fizinė žala kompiuteriams reiškė kompiuterio gedimą, naudojant virusą. Iki tol virusai nebuvo plačiai paplitę, nes internetas buvo skirtas tik gynybos sistemoms, didelėms tarptautinėms kompanijoms ir mokslinių tyrimų bendruomenėms. 1996 m., kai visuomenė galėjo laisvai prieiti ir naudotis internetu, jis iš karto išpopuliarėjo bei pakeitė žmonių gyvenimo būdą (Pande, 2017). Instrukcijos interneto naudotojui buvo parašytos taip aiškiai, kad vartotojui nereikėjo rūpintis, kaip veikia internetas. Interneto vartotojas turi paspausti kelis mygtukus nesijaudinant, kaip šie duomenys yra saugomi arba kur jie gali nukeliauti. Kompiuteriniai nusikaltimai patobulėjo nuo to, kad

buvo apgadintas ar sunaikintas kompiuteris iki manipuliavimo duomenimis vykdant finansinius nusikaltimus. Šios kompiuterinės atakos keičiasi ir tobulėja itin sparčiai.

Internetas įsiskverbė į daugelį žmonių gyvenimo sričių. Žmonės lankosi internete ir naudojasi begalinėmis interneto galimybėmis, internetą naudoja linksmybėms, abipusiam bendravimui, finansinėms operacijoms, bendravimui su valstybinėmis institucijomis ar privačiomis įstaigomis ir pan. Žinių trūkumas apie sukčiavimą internete, duomenų apsaugą bei kitas grėsmes yra saugumo rizikos pagrindas. Būtent dėl šių priežasčių asmenys, institucijos, įmonės dažnai tampa patraukliu kibernetinių nusikaltėlių taikiniu. Problemos, susijusios su kibernetine sauga, tapo dar rimtesnės dėl interneto ryšio. Kenkėjiška programinė įranga, sekimas, virusai, apgaulingi el. laiškai, melagingi skelbimai, neapgalvotas dalijimasis asmenine informacija, el. laiškai su užkrėstomis nuorodomis, asmeninių duomenų, nuotraukų vagystės, o vėliau - šantažas ar patyčios ir pan. vienos dažniausių problemų bei grėsmių naudojantis internetu. Šių rizikų ir grėsmių negalima visiškai pašalinti, tačiau turint žinių ir tinkamą prevencijos formą jos gali būti sumažintos iki priimtino lygio (Lošonczi, 2018).

J. Pande (2017) apibūdina kibernetinį nusikalstamumą kaip neteisėtą veiklą, kai kompiuteris ar tokie kaip išmanieji telefonai, planšetiniai kompiuteriai yra naudojami kaip įrankis ar (ir) nusikalstamo veiksmo taikinys. Autorė taip pat pateikia dviejų rūšių kibernetinių nusikaltimų klasifikaciją:

- Vidinė ataka. Vidinę ataką atlieka asmuo arba asmenys, turinčio prieigą prie sistemos.
- Išorinė ataka. Išorinę ataką atlieka pašalinis žmogus, kuris gali būti pasamdytas, o toks išpuolis vadinamas - išoriniu išpuoliu. Kibernetinės atakos auka tapusi organizacija, įmonė patiria ne tik finansinius nuostolius, tačiau dažnai ir netenkama arba sunaikinama informacija. Tačiau įdiegtos ugniasienės, įsibrovimo aptikimo sistemos, kad būtų galima stebėti išorinius išpuolius padeda apsisaugoti nuo atakų.

A.Klaic (2015) kibernetinę erdvę apibrėžia kaip globalią virtualią aplinką, kurioje yra tarpusavyje sujungtos viešosios ir privačiosios informacinės sistemos. Kibernetinėje erdvėje sukuriama, saugoma ir perduodama įvairių tipų informacija. Skirtingai nuo paprastų elektroninių paslaugų, kurios buvo siūlomos interneto pradžioje, paplitusios visame pasaulyje, šiandienos elektroninė erdvė visiškai pakeitė žmonių privatų ir profesinį gyvenimą, taip pat pakeitė daugumos verslo sektorių infrastruktūrą. Pokyčiai, įvykę per pastaruosius 20 spartaus technologijų vystymosi metų paveikė tiek paprastų žmonių gyvenimo įpročius, tiek verslų. Visos technologijos ir skirtingos paslaugų rūšys nepaprastai palaiko realų globalizacijos procesą pasaulyje ir tuo pačiu tampa būtinybe vyriausybės sektoriui, verslo sektoriams ir piliečiams visose pasaulio

šalyse. Tokiu būdu sparti technologijų plėtra įnešė didžiulius pokyčius verslo procesuose ir piliečių gyvenimo būdui, darantį didelę įtaką ne tik technologijai, kaip vienam svarbiausių visų saugumo politikos veiksnių, bet ir procesams, žmonėms. Tokia nauja virtuali žmonių gyvenimo pasirinkimo galimybė sukėlė tam tikras grėsmes ir išpuolius, tačiau taip pat sukčiavimo ir vagysčių galimybes. Daugelis interneto vartotojų ir infrastruktūrų kiekvieną dieną tampa vis labiau veikiami įvairių kibernetinių grėsmių. Tai lemia daugybė veiksnių, kurie šiandien apibūdina elektroninę erdvę. A.Klaic (2015) išskyrė pagrindinius veiksnius:

- didėjanti kompiuterinių technologijų priklausomybė;
- kompiuterių vartotojų nepakankamas supratimas apie saugumą ir privatumą;
- platus programinės įrangos, kurią galima naudoti kompiuterinėms atakoms, prieinamumas;
- naujų rūšių grėsmės dalyvių įvairovė elektroninėje erdvėje
- valstybės sienų nebuvimas vykdant kibernetines atakas ir asimetriškas kibernetinių išpuolių pobūdis, taip pat;
- nepakankamas vyriausybių ir tarptautinių institucijų pasirengimas ir koordinavimas šiam virtualiam visuomenės aspektui - elektroninei erdvei.

Tačiau kibernetinio saugumo raida prasidėjo gerokai prieš šalims kuriant nacionalines kibernetinio saugumo strategijas. Tarptautinės teisės ir kibernetinio saugumo užduotis yra užtikrinti tarptautinį saugumą, kuris patikėtas įgyvendinti Jungtinių Tautų (JT) organizacijai. JT organizacija pasirašė Jungtinių Tautų chartiją 1945 m. birželio 26 d . Jungtinių Tautų chartijoje pabrėžiama vienas iš JT tikslų - palaikyti tarptautinę taiką ir saugumą. Jungtinės Tautos institucionalizavo ir įkūrė viena iš pagrindinių savo organų – Saugumo taryba. Saugumo tarybos pagrindinė atsakomybė - tarptautinės taikos palaikymas ir saugumas. Nuo šios organizacijos įkūrimo praėjo daugiau nei septyniasdešimt metų, o tarptautinė bendruomenė ir atskiros valstybės dar ir dabar susiduria su įvairiais naujais iššūkiais ir saugumo grėsmėmis, kurios skiriasi nuo tų, kurios buvo žinomos JT įkūrimo metu. Įvairūs autoriai pabrėžia, jog nėra atlikti esminiai pakeitimai Jungtinių Tautų chartijoje.

Per daugiau nei 75 metus atlikti tik smulkūs pakeitimai neatsižvelgiant į kintančias grėsmes, jų mąstus bei pobūdžius nors pakeitimų priėmėjai ir supranta vykstančius pokyčius. To pasekoje atliekami tyrimai, saugumo analizės, rengiami skirtingos tesinės galios tarptautiniai dokumentai. Vienas iš dokumentų, pavyzdžiui, ataskaita susijusi su tarptautinio saugumo klausimu pavadinimu „Saugesnis pasaulis: mūsų bendra atsakomybė“ (2004), kurią parengė tuometinio JT generalinio sekretoriaus Kofi Annan specialistų komanda. Ataskaitoje teigiama, kad gyvename naujų grėsmių pasaulyje, kurios negalėjo

būti žinomos ar numatomos tuo metu, kai buvo įsteigtos Jungtinės Tautos. Autoriaus Jozef Valuch (2017) pavadintoje „Naujojo tūkstantmečio pradžios ataskaitoje“ aprašytos šešios rimčiausios tarptautinės grėsmių kategorijos: tarpvalstybiniai konfliktai, smurtas valstybėse, ekonominės ir socialinės grėsmės, masinio naikinimo ginklai, terorizmas ir tarptautinis organizuotas nusikalstamumas.

Praėjus daugiau nei dešimtmečiui pažanga naujų technologijų srityje ir jų prieinamumas verčia susimąstyti, ar ataskaitoje pateiktos grėsmės vis dar yra aktualios bei tendencingos. Keli įvykiai iš pastarųjų metų patvirtina, kad tarptautinė bendruomenė vėl susiduria su naujais iššūkiais (Pardini, Heinisch, Parreiras, 2017). Prieinamumas, anonimiškumas ir „erdvinis neapčiuopiamumas“ naudojantis informacinėmis technologijomis lemia tai, kad vis daugiau grėsmių kyla kibernetinėje erdvėje, juo labiau neesant baudžiamojo persekiojimo rizikai. Kibernetinė erdvė daugeliu atžvilgių skiriasi nuo bet kokios anksčiau žinomos ir eksploatuojamos erdvės. Ilgą laiką žmonija iš esmės naudojo tik du matmenis - Žemės paviršius ir vanduo (t. y. jūra). Vėliau buvo pridėtos technologijos, dangus ir kosminė erdvė. Dabar be šių keturių dimensijų, yra ir penktasis, tarptautiniams konfliktams - elektroninė erdvė. Jozef Valuch (2017) nuomone, šis penktasis erdvinis matmuo labai skiriasi, palyginti su anksčiau išvardytais pavyzdžiais kadangi gali veikti kaip fizinis asmuo, grupė ar net valstybė. J. Valuch teigimu, pirmose keturiose matmenyse, norint užgrobti kiekvieną plotą, reikėjo pakankamai karinių ir materialinių pajėgumų. Pavyzdžiui, norint užtikrinti pranašumą jūroje, reikėjo disponuoti vyraujančia jūrų galia. Tuo tarpu elektroninėje erdvėje to beveik nėra, nes neįmanoma net per trumpą laiką pasiekti absoliučios hegemonijos - atsižvelgiant į dalyvių skaičių, paprastą prieigą bei anonimiškumą. Galiausiai taip pat labai sunku nustatyti kibernetinės atakos šaltinį. Be visų šių priežasčių šio tipo erdvė taip pat siūlo daugybę galimybių elektroninims nusikaltimams ar kibernetinėms atakoms, apimančioms daugybę neigiamų reiškinių įskaitant kibernetinį karą. Gali būti ir kitų neigiamų kibernetinių atakų pavyzdžių įskaitant ir elektroninį šnipinėjimą, įsilaužimą, paskirstytą paslaugos trikdymo ataką (DDoS išpuoliai) ar kita nepageidaujama veikla, įskaitant ekstremizmą ir piktnaudžiavimą internetu teroristinei veiklai ir teroristų propagandai (pvz., pateikiant sprogmenų gamybos vadovus) ir panašiai.

Šiame kontekste vyksta ilgalaikės diskusijos dėl tarptautinės teisės pritaikomumo elektroninėje erdvėje. Dauguma vakarų šalių palankiai priima galiojančią tarptautinę teisę. Kai kurios kitos šalys, kaip Rusija ir Kinija, pasiūlė įvesti konkretų standartų rinkinį. Vis dėlto galima daryti išvadą, kad visuotinai pripažįstama, jog tarptautinė teisė ir ateityje taip pat turėtų būti taikoma elektroninėje erdvėje. Tai patvirtina 2013 m. Jungtinių Tautų įsteigtos Generalinės asamblėjos vyriausybinių ekspertų grupės ataskaita. Jame teigiama, kad tarptautinė teisė, ypač Jungtinių Tautų chartija yra taikoma ir yra būtina palaikant taiką, stabilumą ir atvirų, saugių, taikių ir prieinamų IKT priemonių aplinką ir taikymą. Tačiau taip pat kyla

klausimas, kaip šiame sektoriuje taikyti tarptautinę teisę, ir tai nėra diskusija, kuri bus lengvai išspręsta artimiausiu metu. Šiuo metu Jungtinių Tautų vadovai nėra sutarę dėl tarptautinės teisės. 2015 m. ekspertų grupei (GGE) buvo pavesta peržiūrėti tarptautinės teisės normas, kurios atsakingos už kibernetinių konfliktų sprendimus. Tačiau diskutuoti šia tema šalims parsirodė labiausiai sudėtinga. Nesutarimai vyravo tarp Rusijos, Kinijos ir keleto kitų šalių (Cornisg, Kavanagh, 2019).

NATO yra tarptautinė karinio ir politinio pobūdžio organizacija, kuri suburia šalis bendradarbiavimui saugumo srityje. NATO kolektyvinė gynyba teikia valstybėms narėms apsaugą politinėmis ir karinėmis priemonėmis. Taigi naujos grėsmės formos negali būti įgyvendintos nepastebėtos organizacijos. Pastaruoju metu svarstomi įvairūs strateginiai dokumentai, kurie apima elektroninę erdvę kaip nauja dominuojanti sritis. Galima paminėti, pavyzdžiui, „NATO Strateginė koncepcija“, priimta 2010 m. Lisabonos viršūnių susitikime. Pagal šią koncepciją kibernetiniai išpuoliai yra viena iš pagrindinių grėsmių šiomis dienomis. Kibernetiniai išpuoliai įvyksta vis dažniau ir sugeba pasiekti tokį lygį, kuris kelia grėsmę nacionaliniam ir euroatlantiniam klestėjimui, saugumui ir stabilumui. Tokių išpuolių dalyviai gali būti užsienio kariškiai ir žvalgybos tarnybos, teroristų ir ekstremistų grupuotės, taip pat organizuotos nusikalstamos grupuotės arba pavieniai nusikaltėliai.

2011 m. NATO priėmė „NATO kibernetinės gynybos politiką“. Dokumentas apibrėžia NATO vaidmenį ir veiklą kibernetinės gynybos srityje. Be šios politikos, buvo priimtas „NATO kibernetinės gynybos veiksmų planas“, kuriame pateikta informacija apie užduotis ir išteklius, kurie leistų pasiekti kibernetinės gynybos tikslus. Planas buvo atnaujintas 2014 m. gegužės mėn. Plane buvo nustatytos konkrečios užduotys, kurios padėtų įvykdyti minėtą politiką, o viena iš pagrindinių užduočių - stiprinti tarpusavio bendradarbiavimą tarp valstybinių, privačių sektorių ir akademinės bendruomenės.

Poreikis užtikrinti kibernetinį saugumą kyla ir ES. Vienas naujesnių ES dokumentų pavadintas „Europos Sąjungos kibernetinio saugumo strategija: atvira, saugi ir patikima kibernetinė erdvė“ (2013), kuris atspindi ES viziją, susijusią su kibernetinės veiklos prevencija, sutrikimais ir išpuoliais, taip pat atsižvelgiant į galimas atsakomąsias priemones. Visų pirma siekiama padidinti informacinių sistemų atsparumą kibernetinėms problemoms, atakoms ir išpuoliams, stiprinti ES tarptautinio kibernetinio saugumo ir kibernetinės politikos gynybą. Šis dokumentas taip apibūdina kibernetinę saugą. Kibernetinis saugumas paprastai reiškia apsaugos priemones ir veiksmus, kurie gali būti naudojami apsaugoti kibernetinę sritį tiek civilinėje, tiek karinėje srityje nuo grėsmių, susijusių su / arba galinčiomis pakenkti tarpusavyje priklausomiems tinklams arba infrastruktūrai. Kibernetinis saugumas siekia išsaugoti tinklų prieinamumą ir informacijos juose konfidencialumą bei infrastruktūros vientisumą. Reaguodama į tai, gynybos ministrai patvirtino ES kibernetinės gynybos politiką. Pagrindiniai jos tikslai yra remti

kibernetinės gynybos plėtrą valstybėms narėms, remti misijas ir jungtinės gynybos operacijas, saugumo politiką, mokslą ir tyrimus.

Svarbus šiuo atžvilgiu yra elektroninės erdvės saugumas, kuris turėtų būti vienas iš pagrindinių ES užsienio politikos prioritetų. Vienas iš naujausių Europos Komisijos veiksmų yra išleisti įstatymai kibernetinio saugumo užtikrinimui - Europos Parlamento direktyva (ES) 2016/1148 ir 2016 m. liepos 6 d. Tarybos sprendimas dėl aukšto bendro lygio Europos Sąjungos poreikio užtikrinti kibernetinį saugumą . Be abipusio bendradarbiavimo direktyvoje reikalaujama, kad kiekviena valstybė narė patvirtintų nacionalinę tinklo strategiją, kuri leistų užtikrinti informacijos saugumą, įsteigtų nacionalinę instituciją, atsakingą už tinklų ir informacinių sistemų saugumą, ir sudarytų grupę, kuri atsakytų už kibernetinių grėsmių prevenciją bei užkardymą, vadinamoji CERT (reagavimo į ekstremalias situacijas komanda).

Vienas iš naujausių JAV dokumentų, susijusių su kibernetinėmis grėsmėmis, pristatytas 2015 m. rugsėjo mėnesį Nacionalinės žvalgybos direktoriaus James R. Clapper pavadinimu „Visuotiniai kibernetiniai pavojai“. Be kita ko, šis dokumentas teigia, kad kibernetinių grėsmių dažnis, rafinuotumas ir rizika didėja, kaip ir intensyvumas. Be to, kibernetinių grėsmių, išpuolių, spektras, metodai, taikiniai ir aukos taip pat plečiasi. Tikėtina, kad ateityje bus tęsiami bandymai pažeisti kompiuterines ir informacines sistemas, tačiau JAV „katastrofiškas išpuolis“ yra mažai tikėtinas. JAV nesitiki „kibernetinio Armagedono“, kuris paralyžiuotų visą JAV infrastruktūrą, tačiau tikimasi išpuolių žemesniu ar vidutiniu lygiu iš skirtingų šaltinių. Šis dokumentas išskiria šiuos kibernetinių išpuolių prieš JAV veikėjus:

a) valstybės, turinčios labai sudėtingas kibernetines programas (pvz., Rusija ar Kinija),

b) valstybes, turinčias mažesnes technines galimybes (pvz., Iranas ar Šiaurės Korėja),

c) pelno siekiantys nusikaltėliai,

d) ideologiškai motyvuoti ekstremistai ar įsilaužėliai.

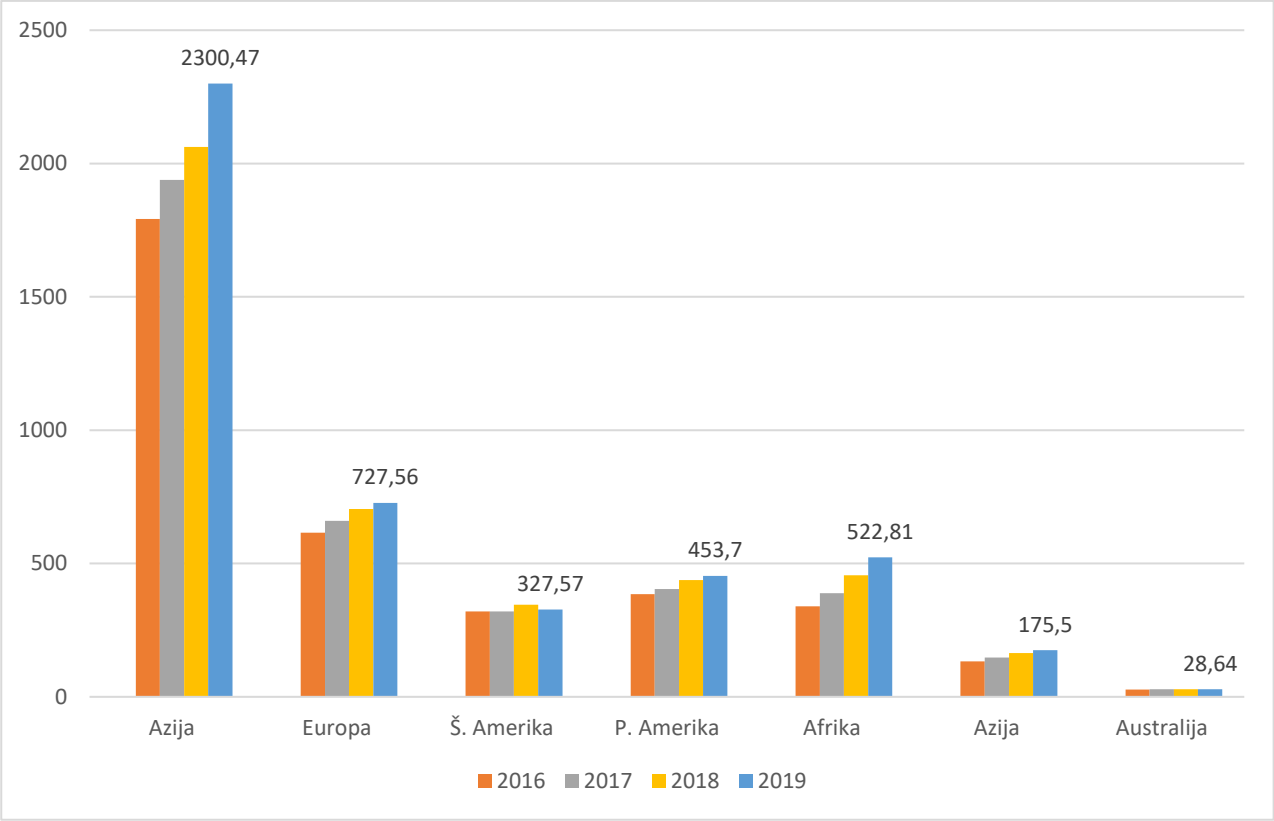
Apibendrinant galima teigti, jog augant kompiuterinių ir ryšių technologijų plėtrai, didėjant poreikiams ir plėtojant informacinių sistemų saugumą pasaulis priverstas susidurti su tam tikromis rizikomis ir viena iš jų – kibernetinis saugumas (Schjolberg, Ghernaouti-Helie, 2009). Kibernetinio saugumo problemą reikia spręsti (Irandoost, 2018). Tobulėjant kompiuterinėms ir ryšių technologijoms, sukurta daugybė informacijos apsaugos priemonių. Įrankių, procedūrų, politikos ir sprendimų, skirtų apsisaugoti nuo atakų – visu tuo galima naudotis, nors linkstame prie to, jog tai remiasi į kaštus. Būtina apibrėžti atakos, rizikos, grėsmės, pažeidžiamumo ir turto vertės sąvokas ir jas sužinoti. Kuriant ir diegiant informacines sistemas pirmiausia reikėtų atsižvelgti į priemonių, skirtų saugumui ir priežiūrai padidinti priimtinu rizikos lygiu rinkinį (Stočis ir Veličkovic, 2013). Bet kokiu atveju reikia žinoti informacinės

sistemos riziką. Potencialūs saugumo šaltiniai tai pat turi tam tikrų iššūkių (gali remtis į finansinius aspektus, ekpertus ir pan.).

1.2 Kibernetinio saugumo aktualumas

Kibernetinis saugumas vaidina svarbų vaidmenį užtikrinant žmonių saugumą, kurie kasdieniame gyvenime naudojasi internetu. Naudodamiesi internetu žmonės susiduria su įvairiomis problemomis. Piktnaudžiavimas internetu tampa aktualia problema įvairiuose sektoriuose: socialinėje žiniasklaidoje, privačiame versle, universitetuose ir vyriausybinėse organizacijose. Dėl greito informacijos ir ryšių technologijų tobulėjimo bei vis didesnio naudojimo daugėja dalinimasis informacija, jos talpinimas, keitimasis, siuntimas bei gavimas, tačiau tuo pačiu metu būtina sutelkti dėmesį į duomenų apsaugą informacinėse sistemose. Kibernetinių atakų sukelėjai nuolatos ieško naujų būdų, kaip užpulti informacines sistemas. Tai kelia pavojų ne tik kompiuterinių sistemų patikimumui, vientisumui ar prieigai, bet ir svarbiausių valstybės infrastruktūrų saugumui. Technologinė plėtra, be kita ko, suteikia erdvės nusikalstamai veiklai šioje srityje. Kibernetinis saugumas yra nuolatinio ir planuojamo politinio, teisinio, ekonominio, saugumo, gynybos ir švietimo sąmoningumo didinimo sistema, taip pat apimanti priimtų ir taikomų techninio-organizacinio pobūdžio rizikos kontrolės priemonių efektyvumą elektroninėje erdvėje, kad paversti ją patikima aplinka, užtikrinančia saugų socialinių ir ekonominių procesų veikimą priimtinu rizikos lygiu elektroninėje erdvėje (Lošonczi, 2018).

Šiais laikais internetas tapo esmine kasdienio gyvenimo dalimi, o ne prabanga. Nuo 2016 iki 2019 m. visame pasaulyje interneto vartojimas augo, ypač išaugo socialinių tinklų, socialinės žiniasklaidos vartojimas (2 pav.). Sparčiai didėjant mobiliųjų įrenginių naudojimui, moksliniai tyrimai buvo skirti nustatyti įvairius šių prietaisų panaudojimo būdus. Nustatyti iššūkiai yra saugumas, elektroninės patyčios, autorių teisės ir plagiatas (Almarabeh, Sulieman, 2019). Vis didėjantis pasitikėjimas socialiniais tinklais visame pasaulyje tapo ypač ryškus pastaraisiais dešimtmečiais dėl jo didelės vertės visais profesinio ir asmeninio gyvenimo lygiais, keliančio produktyvumą ir sprendžiant problemas bei palengvinančiu gyvenimo būdą.

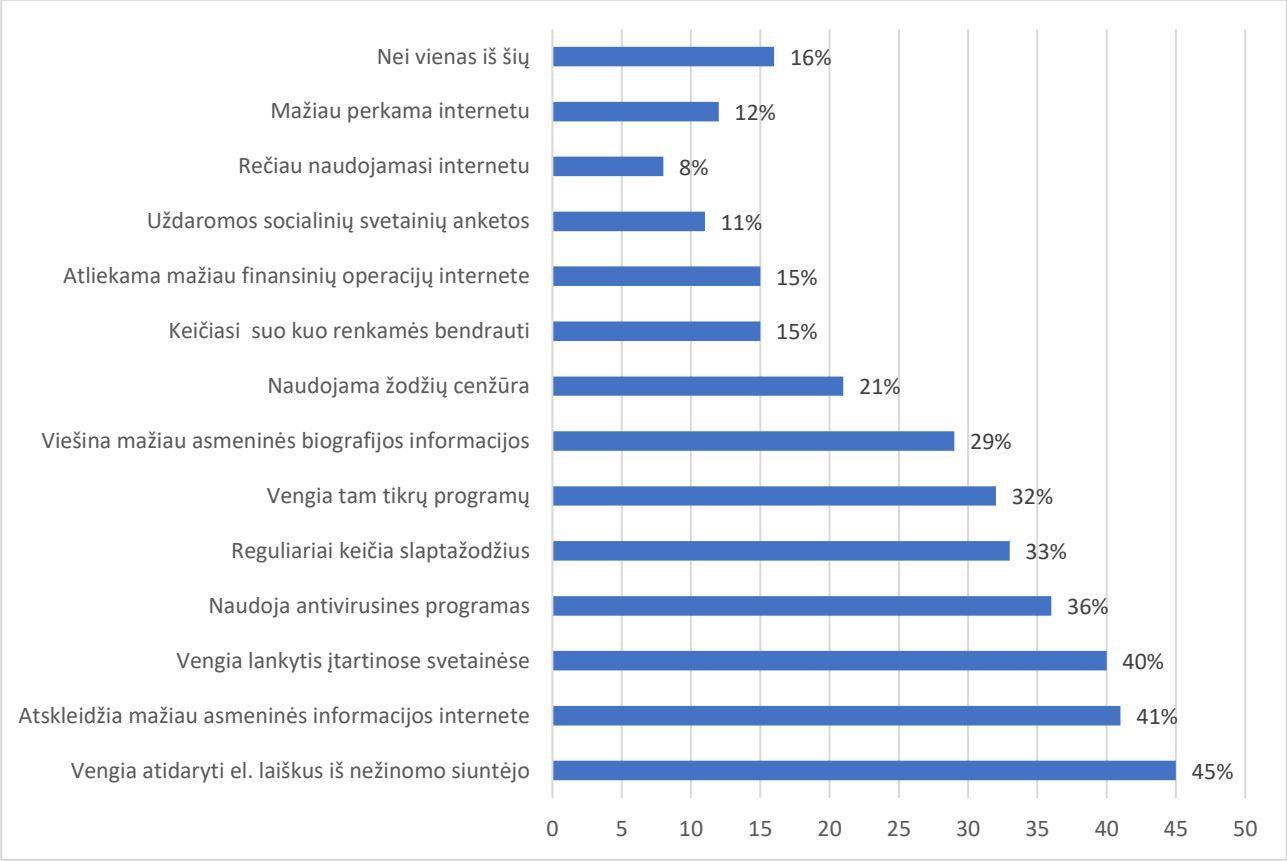


3 pav. Interneto vartotojai 2016-2019 m. pagal regionus (milijonais)

Šaltinis: Statistikos duomenų bazė www.statista.com, 2020

Žmonių sąveika tampa vis labiau priklausoma nuo tiesioginio ir nenutrūkstamo bendravimo per internetą apskritai ir ypač socialinių tinklų svetaines, be el. pašto, informacijos mainų, e. mokymosi ir įvairių kitų programų bei naudojimo būdų profesinėse ir kitose srityse. Populiarėjant mobiliesiems įrenginiams ir programoms, kartu su socialinių tinklų technologijomis, bendravimas naudojant internetines socialinio tinklo priemones tapo nauju žmonių gyvenimo būdu. Dėl didėjančio poreikio valdyti informacines technologijas išaugo grėsmės, kurios trukdo progresui ir neleidžia visiškai kontroliuoti duomenų ir informacijos. Kenkėjiškos programos išplito įvairiais būdais ir nuolat tobulėja dėl savo sudėtingumo, todėl sunku sustabdyti neigiamą ir dažnai destruktyvų jų poveikį. Duomenų vagystė pastaraisiais metais išaugo tiek instituciniu, tiek privačių vartotojų lygmeniu. Naudodamiesi socialinių tinklų paslaugomis, vartotojai dažnai rizikuoja savo asmenine informacija; pavyzdžiui, vartotojai yra linkę naudoti nesaugias programas, piktnaudžiauti įmonių kompiuteriais, prisijungti prie nesaugių tinklų ir keistis neskelbtinais duomenimis šiuose tinkluose. Pastaraisiais metais pastebimai padidėjo socialinių tinklų naudojimo lygis visame pasaulyje. Pavyzdžiui, „Facebook“ dabar apsilanko 2,25 milijardai aktyvių vartotojų kas mėnesį, todėl vartotojų duomenų piratavimo ir tokios informacijos privatumo problema yra

labai svarbi. Socialinių tinklų vartotojų sąveika yra pagrindinis veiksnys, lemiantis daugelį internetinių tendencijų, nesvarbu, ar jos būtų komercinės, profesinės, socialinės ar kitokios. Be to, daugelis įmonių, institucijų ir asmenų išmoko naudotis socialiniais tinklais, tokiais kaip „Facebook“, „Twitter“ ir „LinkedIn“, kad galėtų bendrauti su kolegomis ir klientais (Almarabeh, Sulieman, 2019). Dėl šio spartaus socialinių tinklų svetainių naudojimo išaugo grėsmė, pavyzdžiui, kenkėjiška programinė įranga, kompiuteriniai virusai ir šnipinėjimo programos, nukreiptos į konfidencialumą ir duomenų saugumą. H. Almarabeh ir A. Sulieman (2019) straipsnyje “The impact of cyber threats on social networking sites” aprašė grėsmių tipus. Yra dvi interneto ir socialinių tinklų grėsmių rūšys: klasikinės grėsmės ir šiuolaikinės grėsmės. Anot autoriaus (Almarabeh ir Sulieman, 2019), klasikinės grėsmės: apsimetinėjimas kitu, kenkėjiškos programos, svetainių atakos, DDoS atakos; šiuolaikinės grėsmės yra susijusios tik su internetinių socialinių tinklų vartotojais, tik dėl internetinių socialinių tinklų infrastruktūros, kuri gali pakenkti vartotojų privatumui ir saugumui.



4 pav. Apsaugos priemonės, kurių per pastaruosius metus nuo 2019 m. vasario mėn. ėmėsi interneto vartotojai

Šaltinis: Statistikos duomenų bazė www.statista.com, 2020

CIGI-IPSOS pasaulinis tyrimas “Internet security and trust” atliktas 2018 m. gruodžio 21 d. – 2019 m. vasario 10 d., kurį atliko „Ipsos“ Tarptautinio valdymo inovacijų centras atskleidė interneto vartotojų nuomonę apie pasitikėjimą internetu bei jo apsauga. Tyrimas buvo atliktas 25 šalyse: Australijoje, Brazilijoje, Kanadoje, Kinijoje, Egipte, Prancūzijoje, Vokietijoje, Didžiojoje Britanijoje, Honkonge (Kinija), Indijoje, Indonezijoje, Italijoje, Japonijoje, Kenijoje, Meksikoje, Nigerijoje, Pakistane, Lenkijoje, Rusija, Pietų Afrikoje, Korėjos Respublikoje, Švedijoje, Tunise, Turkijoje ir JAV. Tyrime dalyvavo 25 229 interneto vartotojai. Dvidešimt viena šalis pasirinko „Ipsos“ interneto sistema, o keturios (Kenija, Nigerija, Pakistanas ir Tunisas) naudojo tiesioginius pokalbius, atsižvelgiant į šių šalių internetinius suvaržymus ir apklausos trukmę. Vidutinė internetinės apklausos trukmė (interviu trukmė) buvo apie 10 minučių. Vidutinis tiesioginių pokalbių laikas buvo maždaug 20 minučių ar daugiau. JAV ir Kanadoje respondentai buvo 18–64 metų, o visų kitų šalių gyventojai - 16–64 metų amžiaus. Kiekvienoje šalyje buvo ištirta maždaug 1000 ir daugiau asmenų.

Aštuoni iš dešimties apklaustųjų susirūpinę savo privatumu internete. Vienas iš penkių apklaustųjų teigia, kad darosi sunkiau naršyti internete tikint, kad turinys nėra cenzūruojamas. Tyrimo dalyviai išreiškė susirūpinimą dėl privatumo internete, dalyvių nuomone tai tiek užsienio valstybių, tiek šalies vidaus kaltė. Vienas iš keturių pasaulio piliečių nepasitiki internetu, nepasitikėjimą vis labiau kursto socialinė žiniasklaida, vyriausybės ir paieškos sistemos. Dėl nepasitikėjimo internetu atskleidžiama vis mažiau informacijos, selektyviau naudojamasi internetu ir, be kitų atsargumo priemonių, perkama vis mažiau internete.

Dvidešimt pirmojo amžiaus pradžioje pastebimai padidėjo interneto ir socialinės žiniasklaidos programų augimas ir plėtra. Todėl padidėja vartotojų sąveika socialinėje žiniasklaidoje naudojant skirtingas internetines programas. Augant šiam skaičiui, iškilo daugybė grėsmių, leidžiančių konfidencialiai įsiskverbti į vartotojų duomenų apsaugą. Šios grėsmės tapo vienu iš iššūkių kurios stengiasi neutralizuoti kibernetinio saugumo specialistai.Kadangi pažeidūs vartotojų duomenis per įsiskverbimą į internetinius socialinius tinklus, duomenys gali patekti pašaliniams vartotojams, paslaugų teikėjams ir kitiems asmenims, kurie savo verslui naudoja internetinių socialinių tinklų duomenis. Šiame darbe buvo paaiškintos įvairios apsaugos ir privatumo problemos, susijusios su internetinių socialinių tinklų vartotojais ir duomenimis. Pagrindinis šio tyrimo tikslas - išryškinti grėsmes, kylančias iš socialinės žiniasklaidos, ir šviesti internetinių socialinių tinklų vartotojus, kaip apsaugoti save ir savo duomenis nuo šių grėsmių, kai jie naudojasi socialine žiniasklaida.

Informacijos infrastruktūrą sudaro technologijos ir galimybės rinkti, tvarkyti ir keistis informacija, kuria dalijasi arba kuria paprastai naudojasi kelios organizacijos, nepriklausomai nuo to, ar jos yra vienos

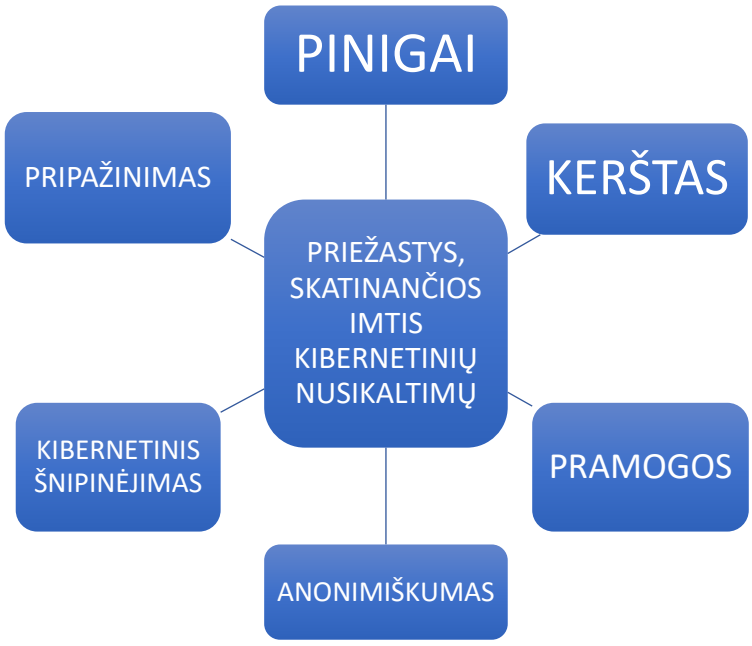
įmonės, ypatingos svarbos infrastruktūros sektoriuje, tokiame kaip bankininkystė ir finansai, vyriausybės, visos šalies ar tarptautiniu mastu. Beveik kiekvienas šiuolaikinio gyvenimo aspektas asmenims, įmonėms ir vyriausybėms tam tikru būdu priklauso nuo informacinės infrastruktūros. Verslas, būtiniausių paslaugų teikimas, nacionalinis saugumas, laisvalaikis ir asmeninių reikalų tvarkymas vis labiau priklauso nuo mūsų sugebėjimo susisiekti ir bendrauti su žmonėmis bei aplinka naudojantis informacinėmis technologijomis.

Per pastaruosius dešimt metų pastebimas reikšmingas informacinė infrastruktūros išplitimas, atsirado padidėjusi priklausomybė nuo IKT ir aplinkos, kurioje jos yra kuriamos, naudojamos. Vis dėlto informacinė infrastruktūra yra pažeidžiama: gedimai, atakos, išpuoliai bei kitokio pobūdžio grėsmės. Informacijos infrastruktūros pažeidžiamumas kyla iš daugelio šaltinių, įskaitant būdingą naujųjų technologijų saugumo trūkumą, dažniausiai naudojamų gaminių trūkumus ir organizacines nesėkmes šalinant sistemos projektavimo ir naudojimo saugumo problemas.

Saugumui grėsmę kelia įvairūs asmenys - nuo paauglių, įsilaužiančių į sistemas, siekiančių girtis iki nusikalstamų organizacijų ir teroristų, kurie siekia padaryti žalą nuo šalies vidaus iki užsienio šalių, vykdant šnipinėjimą ar karines operacijas. Išpuolių metodai išskiriami į keturias grupes:

- fiziniai (bombos);
- socialiniai (gandai, dezinformacija);
- kibernetiniai (žala informacinėmis technologijomis) arba jų derinys.

J. Pande (2017) išskiria priežastis, kurios skatina imtis kibernetinių nusikaltimų (4 pav.).



5 pav. Priežastys, skatinančios imtis kibernetinių nusikaltimų

Šaltinis: Pande, adaptuota pagal autorių, 2020

J. Pande (2017) išskyrė šešias priežastis, kurios skatina imtis kibernetinių nusikaltimų. Viena pagrindinių priežasčių – pinigai. Tačiau kai kuriuos asmenis motyvuoja kerštas. Kai kurie žmonės bando atkeršyti asmeniui, organizacijai, visuomenei, kastai ar religijai, šmeižiant jų reputaciją arba sukeliant ekonominius ar fizinius nuostolius. Taip pat dalis žmonių daro kibernetinius nusikaltimus dėl pramogos. Mėgėjas, autorės nuomone, daro kibernetinius nusikaltimus savo malonumui, o kai kurie asmenys siekia pripažinimo, nulaužiant kompiuterius ar tinklus. Viena iš priežasčių taip pat įvardijama - anonimiškumas. Daugeliu atvejų anonimiškumas, kurį suteikia elektroninė erdvė, motyvuoja žmogų įvykdyti nusikaltimus. Kibernetiniame pasaulyje daug lengviau atsikratyti nusikalstamos veiklos nei realiame pasaulyje. Šeštoji priežastis - kibernetinis šnipinėjimas. Anot autorės kartais vyriausybė pati užsiima elektroninių nusikaltimų vykdymu, kurią motyvuota politinės, ekonomikos ir socialinės priežastys.

Grėsmė informacinei infrastruktūrai ir toliau auga. Todėl pastaraisiais metais pagrindinis dėmesys skiriamas moksliniams tyrimams ir plėtrai, siekiant apsaugoti informacinę infrastruktūrą nuo kibernetinių grėsmių. Dėl šalių priklausomybės nuo informacijos ir kompiuterinių tinklų ryšių, duomenų valdymo ir ypatingos svarbos infrastruktūros objektų veikimo, kibernetinės erdvės tampa vis labiau pažeidžiamos kompiuterinių ar kibernetinių atakų sistemos. Kibernetinės atakos dabar kelia grėsmę ne tik informacinei infrastruktūrai, bet ir kitoms kritinėms infrastruktūroms, tokioms kaip bankai ir finansai, transportas ir energetika, kurios priklauso nuo informacinių technologijų. Be to, kadangi šios infrastruktūros yra labai susijusios, atakos prieš vieną infrastruktūrą gali pakenkti ir kitoms infrastruktūroms. Taigi sutelktos infrastruktūros atakos gali turėti reikšmingą poveikį nacionaliniam saugumui ir ekonomikai.

Kaip rašoma Kibernetinio saugumo tyrimų ir plėtros darbotvarkėje (2003) svarbu tai, kad problema neapsiriboja paaugliu, kuris puola sistemas tik dėl iššūkio. Atvirkščiai, pastaraisiais metais padaugėjo atakų iš daug sudėtingesnių veikėjų, tokių kaip organizuotas nusikalstamumas, teroristinės grupuotės ir, svarbiausia, užsienio šalių, kuriančių kibernetinių išpuolių metodus, pradedant šnipinėjimu prieš šalių vyriausybes agentūras. Kaip teigiama naujausioje Gynybos mokslo tarybos ataskaitoje: „Tam tikru metu JAV atakuos ne įsilaužėliai, o sudėtingas priešininkas, naudodamas veiksmingą informacijos karo priemonių ir metodų rinkinį. Galimi du pasirinkimai: prisitaikyti prieš ataką ar po jos".

Kibernetinis saugumas taip pat yra gyvybiškai svarbus saugant asmens privatumą - problema, dėl kurios visuomenės vis labiau jaudinasi. Kibernetinio saugumo tyrimų ir plėtros darbotvarkėje (2003) rašoma, jog Federalinė prekybos komisija pastebėjo, kad amerikiečiams ypač nerimą kelia tapatybės vagystės. Vagys gali pavogti asmeninę informaciją ir sąskaitoms, aukos vardu sukurti naujas paskyras ar vykdyti kitokio pobūdžio sukčiavimą. Kadangi teroristai naudoja asmens tapatybės vagystes, kad

palengvintų jų judėjimą ir operacijas, tai yra viena iš kelių sričių, kuriose privatumo ir nacionalinio saugumo problemos sutampa.

Tačiau nors kibernetinio saugumo problema ir toliau auga, o visuomenės susirūpinimas proporcingai didėja, autorių teigimu techninės gynybos būklės netobulėja. Kibernetinio saugumo tyrimų ir plėtros darbotvarkėje (2003) teigiama, jog didėjantis žinių atotrūkis tarp kibernetinių užpuolikų ir gynėjų leido padaryti išvadą, kad „gynybos departamentas šiandien negali apsiginti nuo informacinių operacijų išpuolio, kurį vykdo sudėtingas nacionalinės valstybės priešininkas“. Neseniai OMB pranešė, kad „daugelis [kitų] agentūrų praktiškai neturi sistemų, leidžiančių patikrinti ar stebėti sistemos veiklą, todėl jos negali aptikti įsibrovimų ar virusų“.

Privatusis sektorius taip pat patiria sunkumus kovojant su kibernetiniu pavojumi. Kai kurios įmonės imasi iniciatyvių priemonių, o kitos naudojasi kur kas primityvesniu saugumu, jei toks yra. Kaip ir vyriausybėje, nė viena įmonė nėra atspari sudėtingam išpuoliui. Net privačios įmonės, kurios naudoja įsilaužimo aptikimo sistemas ir kitas kompiuterio saugumo priemones, mano, kad jų pažeidžiamumas didėja, ir tai patvirtina atakų statistika. Viena vertus, pagrindinės technologijos, kuriomis grindžiamas internetas, nebuvo sukurtos galvojant apie kibernetinį saugumą. Kita vertus, didėjantis informacinių technologijų sudėtingumas didina išpuolių galimybes, todėl šalims skubiai reikia naujų technologijų, kurios nustatytų ir pašalintų pažeidimus, apsaugotų informacijos infrastruktūrą, padarydamos ją tvirtesnę ir atsparesnę atakų akivaizdoje.

Apibendrinant galima teigti, jog šiandien internetas yra sparčiausiai auganti infrastruktūra kasdieniame gyvenime. Šiandieninėje techninėje aplinkoje daugelis naujausių technologijų keičia žmogaus veidą. Tačiau dėl šių besiformuojančių technologijų mes negalime labai efektyviai apsaugoti savo asmeninės informacijos, todėl šiomis dienomis kibernetinių nusikaltimų skaičius auga kasdien. Kaip teigia N. R. Gade ir U. Reddy (2014), šiandien daugiau nei 60 proc. visų komercinių operacijų atliekama internetu, todėl norint užtikrinti skaidrias operacijas, šioje srityje reikia aukštos kokybės saugumo. Taigi kibernetinis saugumas tapo tokia aktuali problema. Kibernetinio saugumo sritis neapsiriboja tik informacijos saugumu IT pramonėje, bet ir įvairiose kitose srityse, tokiose kaip kibernetinė erdvė ir pan. Net ir naujausioms technologijoms, tokioms kaip debesų kompiuterija, mobilusis kompiuteris, elektroninė komercija, internetinė bankininkystė ir kt., taip pat reikia aukšto lygio saugumo užtikrinimo. Kadangi šiose technologijose yra svarbi informacija apie asmenį, informacijos saugumas tapo būtinu dalyku. Kibernetinio saugumo stiprinimas ir ypatingos svarbos informacinės infrastruktūros apsauga yra būtini kiekvienos šalies saugumui ir ekonominei gerovei (Sandar ir Win, 2019). Interneto saugumo užtikrinimas (ir interneto vartotojų apsauga) tapo neatskiriama plėtojant naujas paslaugas ir vyriausybės politiką. Atsižvelgiant į tai,

kad vien techninėmis priemonėmis negalima užkirsti kelio jokiems nusikaltimams, labai svarbu, kad teisėsaugos institucijoms būtų leista veiksmingai tirti kibernetinius nusikaltimus ir patraukti atsakingus asmenis baudžiamojon atsakomybėn. Šiandien daugelis šalių ir vyriausybių taiko griežtus kibernetinius įstatymus, kad būtų išvengta svarbios informacijos praradimo. To pasekoje, tampa ypač svarbu, kad kiekvienas asmuo turėtų bent bazinių žinių apie kibernetinį saugumą.

2. TRANSNACIONALINIO KIBERNETINIO SAUGUMO PADĖTIS

2.1 Patirtis kibernetinio saugumo sektoriuje

Kibernetinė erdvė šiandien tampa neišvengiama visuomenės gyvenimo dalimi. Šalys ir tarptautinės bendruomenės deda daug pastangų, kad užtikrintų tam tikras sąlygas ir atsakomybę šioje erdvėje. Šios sąlygos ir atsakomybė yra panašios į tas, kurias turime fizinėse savo visuomenės srityse. Dėl šio požiūrio daugelis nacionalinių kibernetinio saugumo strategijų, įskaitant Europos Sąjungos (ES) ir Šiaurės Atlanto sutarties organizacijos (NATO) strategijas, per labai trumpą laiką tapo svarbiomis šių dienų politinėmis darbotvarkėmis. Pagrindiniai principai ir strategijos įgyvendinimo būdai kurių reikia laikytis, vis dar išlieka skirtingai nagrinėjami skirtingose šalyse. Tuo pačiu metu daugybė šalių turi panašias vertybes ir lūkesčius, o daugelis iš jų turi narystės ar partnerystės statusą ES ir NATO. Šalims kyla iššūkiai kuriant nacionalines kibernetinio saugumo strategijas, daugiausia dėmesio skiriant labai nevienalyčio kibernetinio saugumo strategijos turinio suderinimui su skirtingais nacionaliniais ir tarptautiniais reikalavimais ir lūkesčiais.

Kaip pirminį pavyzdį galima paminėti 2007 m. balandžio mėnesio atvejį, kai Estija susidūrė su trijų savaičių trukmės paskirstyta paslaugos trikdymo ataka (DDoS išpuoliai). Kaip aprašo R. Ottis (2018) stimulas buvo Estijos valdžios institucijų sprendimas perkelti Sovietų laikų karo memorialą iš sostinės centro į karines kapines. Šis poelgis sukėlė riaušes tarp rusų mažumos, kurios nariai suvokia, jog memorialas yra paminklas karo aukoms, tačiau estai šį paminklą matė kaip užsienio okupacijos simbolį. Tai taip pat paskatino pasipiktinimų bangą prie Estijos ambasados Maskvoje. DDoS išpuoliai pirmiausia buvo nukreipti į vyriausybių įstaigų tinklalapius, o vėliau ir kai kurių pagrindinių laikraščių, TV stočių, bankų tinklalapius ir kitus taikinius. Keletas svetainių turinys buvo pakeistas į Rusijos propagandos skleidimu arba su klaidingu atsiprašymu už tai, kad tinklapiai yra nefunkcionalūs, tačiau dauguma atakų buvo nukreiptos tiesiog į svetainių išjungimą. Estijos gynybos ministerijos atstovas spaudai palygino šiuos išpuolius su JAV 2001 m. rugsėjo 11 dienos. Estija pareiškė, kad įvyko keletas pirmųjų išpuolių iš Rusijos, bet dauguma jų atsirado vėliau iš daugybės tūkstančių paprastų kompiuterių iš viso pasaulio, todėl sunku priskirti atsakomybę pavieniui valstybei-veikėjui (Rusija). Keletoje svetainių patalpinta informacija, kuri skleidė nepasitikėjimu Estijos valdžia, kai kurios svetainės išplatino instrukcijas, kaip atlikti DDoS išpuolius. Dar daugiau atakų buvo nukreipta skleisti ir užkrėsti kompiuterius virusu bei įtraukti juos į šias atakas. Kai kurie šaltiniai tvirtina, kad šiame išpuolių etape dalyvavo daugiau nei vienas milijonas kompiuterių iš daugiau nei šimto šalių. Tačiau iš esmės šie išpuoliai lėmė „tik“ ekonominius ir ryšių sutrikimus ir nesudarė jokio žymaus turto sugadinimo ar praradimo.

2008 m. įvyko Rusijos-Gruzijos konfliktas. Kibernetinės operacijos prieš Gruziją vyko 2008 m. liepos pabaigoje ir rugpjūčio pradžioje prieš ginkluotą konfliktą su Rusija ir jo metu. Kaip rašoma "Rusijos-Gruzijos karas 2008: kibernetinių atakų vaidmuo konflikte" (2012) vyriausybinės svetainės buvo išjungtos, o interneto paslaugų teikimas sulėtėjo. Ypač prieš ir po Rusijos kariuomenės įžengimo į Gruziją Pietų Osetijos provincijoje, kelios vyriausybinės interneto svetainės buvo išjungtos arba jų turinį pakeitė anti gruzinų propaganda, tuo tarpu DDoS išpuoliai užkirto kelią Gruzijos valdžios institucijoms platinti bet kokią informaciją. Gruzija apkaltino Rusijos Federaciją dėl šių kibernetinių išpuolių, bet Rusija tai neigė ir tvirtino, kad išpuolius atliko privatūs asmenys, kurie tai padarė savo noru. Tuo metu šios kibernetinės operacijos buvo nagrinėjamos nepriklausomų ekspertų, tačiau šie kibernetiniai išpuoliai nebuvo pripažinti ir priskirti Rusijai. Ekspertai pareiškė, kad jei išpuolius ir kontroliavo vyriausybės ar vyriausybė, tikėtina, kad šios formos karas pirmą kartą buvo naudojamas tarpvalstybiniame ginkluotame konflikte. Kai kurių šaltinių teigimu, išpuoliai kilo iš penkių anoniminių sistemų: keturios Rusijoje ir viena Turkijoje. Visos anoniminės sistemos tuo metu buvo kontroliuojamas nusikalstamo sindikato.

M. Baezner ir P. Robin 2018 m. aprašo Stuxnet kirmino atsiradimą Irano kompiuteriuose 2010 m. Iranas tapo kibernetinių atakų taikiniu 2010 metais, tai buvo susiję su šalies branduoline programa. Taip buvo vadinamojo kompiuterinio slieko atvejis „Stuxnet", kuris buvo vienas moderniausių ir intelektualiausių kompiuterinių kirminų. Jis buvo aptiktas 2010 m., virusas apibūdinamas kaip lengvai plintantis „Microsoft Windows" ir daugiausia dėmesio skyrė „Siemens" ir jos pramoninei programinei įrangai. Ekspertai ataką vadina gana paprasta. Virusas gali pakenkti ypač svarbiems objektams, pavyzdžiui, programoms, valdančioms ir stebinčioms pramoninius procesus arba bendradarbiaujančios su įvairiomis kitomis sistemomis ir programomis. Iki šiol, žinomi penki skirtingi „Stuxnet" tipai, kurie buvo naudojami prieš iraniečių įrenginius. Dėl šių išpuolių buvo sugadinta Irano branduolinė programa. Tai įrodo tolesnį kokybinį kibernetinių atakų naudojimo žingsnį, nepaisant fakto, kad žalos mastas neaiškus, šis įvykis patvirtina potencialų kenkėjiškų programų, galinčių apimti svarbias kompiuterines sistemas, valdančias energiją, tiekimą ar eismo tinklus tobulėjimą. Taigi ši byla laikoma pirmąja kibernetinės atakos forma nukreipta į išpuolius, galinčius padaryti realią fizinę žalą ir kelti pavojų žmonių gyvybėms. Tuo remiantis galima daryti išvadą, kad „Stuxnet" buvo pirmasis pasaulinis kibernetinis geopolitinės svarbos ginklas. Vis dėlto nė vienas konkretus asmuo ar valstybė nebuvo kaltinamas šiame kibernetiniame kare.

Vienas svarbiausių vėlesnių kibernetinių išpuolių laikomas 2014 m. „Sony Pictures Entertainment" kino studijose, iš kurių buvo pavogta daugybė svarbių dokumentų apie filmus, įžymybes ir prieigos duomenis. Kaip teigia A. DeSimone ir N. Horton (2017) puolimas buvo priskirtas Šiaurės Korėjai dėl to, kad studija rengė filmą, kuriame turėjo mirti Šiaurės Korėjos lyderis. Kitas kibernetinės atakos pavyzdys,

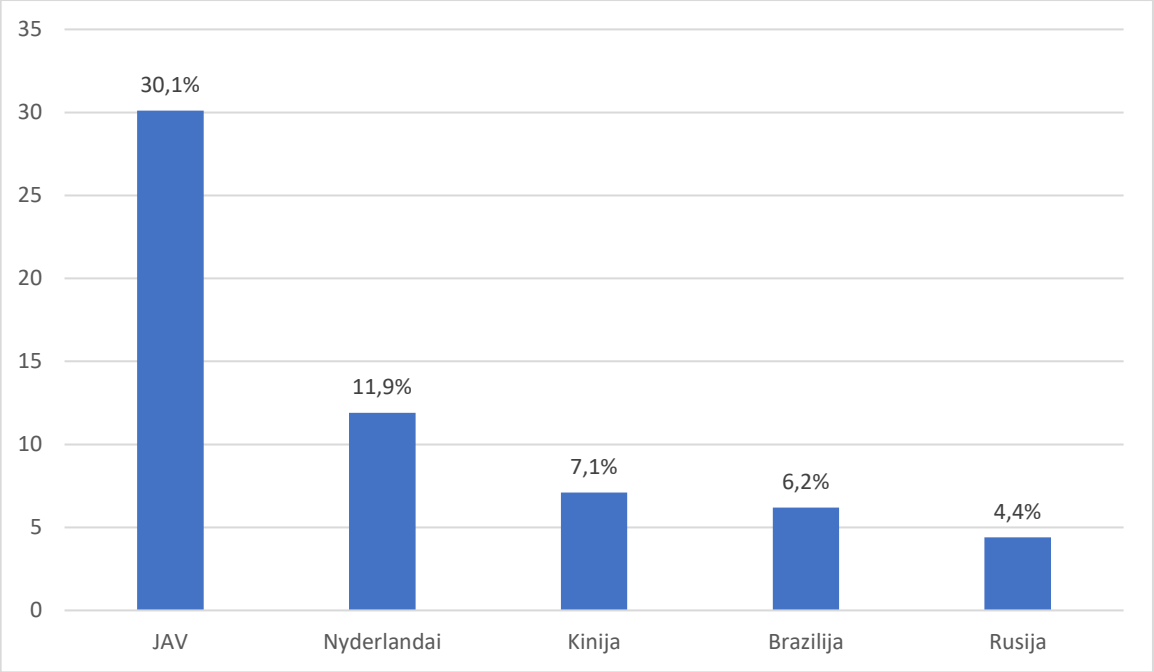
priskiriamas „Islamo valstybei“ (iš tikrųjų veikiau ne valstybei, o ISIS), kuris 2015 m.buvo nukreiptas į „Twitter“ paskyrą ir „YouTube“ kanalą, kurie priklausė Centrinei JAV armijos vadovybei. Centrinė vadovybė yra JAV kariuomenės dalis atsakinga už pasaulio regionus, kuriuose vyksta JAV karinės operacijos t.y., apie dvidešimt šalių, įskaitant Afganistaną, Iraną, Iraką, Saudo Arabiją ir Sirija. Šalia šūkio "Mes nesustosime! Mes viską apie jus žinome" buvo rodomi kariškių vardai ir telefonų numeriai. Socialiniuose tinkluose plito įrašai su žodžiais „Alacho vardu, maloningiausias, dievobaimingiausias „CyberCalifhate“ tęsia savo „CyberJihad“ plėtrą. Centrinės vadovybės „YouTube“ paskyra parodė vyrą su skara bei užrašu „Aš tave myliu ISIS“. Pentagono atstovo teigimu, kad nors tai gėda JAV , neįrodyta, kad tai buvo reali grėsmė saugumui.

M. Baezner ir P. Robin (2018) aprašė 2013 m. prasidėjusią vadinamąją Ukrainos krizę, arba vadinamąją Rusijos-Ukrainos, konflikto pradžią. Apskritai šis konfliktas dažnai vadinamas kaip hibridinis karas - netradicinės taktikos mišinys ir strategijos, slapti veiksmai, kibernetinės operacijos ir politinės manipuliacijos siekiant politinių tikslų. Pasirinkti šalių veiksmai iš esmės atrodo kaip taktikos rinkinys. Įprastinis karas yra tik dalis įvairesnių prievartos veiksmų. Šiuo atveju taip pat buvo naudojamos elektroninės operacijos tokios kaip informacinis karas. Informacinis karas apėmė skaitmeninę propagandą, svetainių išjungimą, informacijos nutekinimą, pažangiausius kibernetinio šnipinėjimo virusus ir panašiai. Tačiau, išskyrus sutrinkusio interneto ryšio tarp Krymo, Donbaso ir kitų Ukrainos miestų nebuvo žinoma jokių išpuolių prieš civilius ar karinę infrastruktūra. Kai kurių autorių teigimu, Rusijos kibernetinė veikla susijusi su nesenu konfliktu Ukrainoje ir Krymo aneksija, ko gero, yra geriausias elektroninių atakų pavyzdys, kai pasitelktas informacinis karas - formuoti bendrą politinę ginčo eigą.

Aukščiau pateikti pavyzdžiai yra tik keletas šiuolaikinių ir netiesioginių konfliktų, susijusių su elektroninės erdvės naudojimu artėjant prie karo lygio, atvejų. Daugybė kitų valstybių turi faktinę panašių intervencijų patirtį. Tai gana natūraliai paskatino tarptautines organizacijas, įvairias organizacijas reaguoti į tokio pobūdžio grėsmę, priimant įstatymus, atsižvelgiant į atitinkamų gebėjimų bei tarptautinio bendradarbiavimo stiprinimą. Kibernetinės operacijos sukūrė rizikingą erdvę, kurioje valstybės gali vykdyti skausmigas pasekmes sukeliančius veiksmus.

Daugybė šalių ir tarptautinių organizacijų pastaraisiais metais įdėjo daug pastangų, kad užtikrintų tam tikras sąlygas ir atsakomybes kibernetinėje erdvėje. Šios sąlygos ir atsakomybės yra panašios į tas, kurias turime fizinėse savo visuomenės srityse. Dėl šios priežasties daugelis iniciatyvų kurti nacionalines kibernetinio saugumo strategijas, įskaitant ES ir NATO strategijas, per labai trumpą laiką tampa svarbia šių dienų politinių darbotvarkių dalimi.

Nepaisant visų šių pastangų, skirtingose šalyse vis dar labai skirtingai nagrinėjami klausimai dėl atsakingų institucijų, į kurias reikia atsižvelgti strategijoje, vadovaujantis pagrindiniais principais ir strategijos įgyvendinimo būdu. Daugybė šalių turi tas pačias vertybes ir lūkesčius, o kai kurios iš jų turi narystės ar partnerystės statusą ES ir NATO. Todėl šie skirtingi nacionaliniai kibernetinio saugumo požiūriai gali būti tam tikros kliūtys tolesniam visuomenės vystymuisi dėl globalizuotos rinkos ekonomikos ir bendrų standartų, kuriuos reikia nustatyti daugelyje skirtingų šalių verslo ir visuomenės sektoriuose. Dabartinis ES pasiūlymas apima ne tik tradicines telekomunikacijų sektoriaus problemas, bet ir daug daugiau sričių (pvz., ypatingos svarbos infrastruktūros objektų apsauga, dalijimąsi informacija ir kt.). Visose ES narėse yra vienodi ar bent jau panašūs kibernetinio saugumo standartai.



6 pav. Visuotinio žiniatinklio programų išpuolių srauto dalis pagal kilmės šalį nuo 2017 m. lapkričio mėn. iki 2018 m. balandžio mėn.

Šaltinis: www.statista, 2020

Statistika rodo procentinę pasaulio šalių interneto atakų srautą nuo 2017 m. lapkričio mėn. iki 2018 m. balandžio mėn. pagal kilmės šalis. Per šį laikotarpį 30,1 proc. atakų kilo iš IP adresų JAV. JAV taip pat buvo šalis, kuriai labiausiai buvo skirtos interneto atakos, kurios per 2017 m. paskutinį ketvirtį patyrė daugiau nei 238,6 mln. išpuolių. 2017 m. vidutinės kibernetinių nusikaltimų išlaidos JAV sudarė 21,22 mln. JAV dolerių, o tai didžiausia išleista suma pasaulyje.

Internetas tapo kritine infrastruktūra tiek verslui, tiek individualiems vartotojams, todėl jo saugumas tapo prioritetiniu klausimu. Saugumas taip pat yra svarbus raktas į šiuolaikinį pasaulį ir lemiamas veiksnys, skatinantis vartotojų pasitikėjimą, būtiną norint pasiekti technologijų sėkmę.

Mūsų didėjanti priklausomybė nuo apsipirkimo internete ir paslaugų gavimo toje pačioje erdvėje padidino kibernetinių grėsmių įvairovę ir kiekį, kuris dabar įsiskverbia į kasdienį žmonių gyvenimą ir kelia grėsmę ekonomikos stabilumui. Pastaraisiais metais buvo pastebėta daugybė saugumo pažeidimų - vieni atsitiktiniai, kiti - tyčiniai, turėję didelį poveikį informacinių ir ryšių technologijų (IRT) sistemoms ir tinklams. Visuotinai pripažįstama, kad vartotojai turi būti apsaugoti, taigi, nors kibernetinių nusikaltimų skaičius vis didėja, taip pat didėja ir pastangos tam pasipriešinti. Prie to prisideda nauji teisės aktai, dokumenti, kurie aptaria saugumo klausimus. C. Brookson (2016) teigimu, kibernetinio saugumo sprendimai priklauso nuo įvairių faktorių - pasitikėjimo, kad klausimai yra tinkamai sprendžiami. Apibendrinant galima remtis W. Gharibi ir A. Mirza (2011) nuomone, kurių teigimu saugumas yra daugialypė sistema, kurią sudaro saugos programinė įranga, paslaugos, politika ir žmogiškasis faktorius. Nė vienas iš jų neturėtų būti praleistas kuriant saugią aplinką.

Drąsiai galima teigit, jog kibernetinis karas ir terorizmas nepažįsta sienų. Veiksmams virtualioje erdvėje reikia atmesti įprastas prielaidas, susijusias su laiku ir erdve, nes tokias atakas naudojant modernius informacijos ir ryšių tinklus galima atlikti iš bet kurios vietos per labai trumpą laiką. Globalizacijos procesai turėjo įtakos civilizacijos plėtrai. Terorizmas ir nacionalinės grėsmės pasikeitė veikiant globalizacijos procesui ir interneto informacijos revoliucijai. Strateginis pranašumas yra nebe kovos galia ar geografinė padėtis, o informacija ir žinios. Tarptautinis bendradarbiavimas ir dalijimasis žiniomis yra būtini norint veiksmingai užkirsti kelią kibernetinėms grėsmėms. O pastaraisiais metais kibernetinės grėsmės buvo ypač pabrėžiamos šiuolaikinėse karinėse didžiųjų valstybių ir NATO doktrinose. I. Duic, V. Cvrtila, T. Ivanjko (2017) teigimu, kibernetinę erdvę siekiama parodyti, atsižvelgiant į saugumo iššūkius, kaip aspektą, kuriame klostosi tarptautiniai santykiai.

2010 m. Lisabonos viršūnių susitikime priimtoje NATO strateginėje koncepcijoje nustatyta, kad kibernetinės atakos tapo vis dažnesnės, labiau organizuotos ir brangesnės, o tai daro žalą įvairiems sektoriams. Taip pat teigiama, kad kibernetinės atakos gali pasiekti tokį lygį, kuris kelia grėsmę nacionaliniam ir euroatlantiniam klestėjimui, saugumui ir stabilumui. Užsienio šalių karinės žvalgybos tarnybos, organizuoti nusikaltėliai, teroristai ir ekstremistinės grupės yra potencialūs tokių išpuolių šaltiniai. Lisabonos aukščiausiojo lygio susitikimo išvadose taip pat pabrėžiama būtinybė toliau plėtoti prevencijos, pripažinimo, gynybos ir atkūrimo po kibernetinių išpuolių įgūdžius, įskaitant NATO planavimo proceso naudojimą siekiant stiprinti ir koordinuoti nacionalinius piliečių sugebėjimus.

Reikėtų nepamiršti, kad spartus technologijų vystymasis ir jos pritaikymas kasdieniame gyvenime užpuolikams atveria daug galimybių, nesvarbu, ar jie būtų valstybių, teroristų ar nusikaltėlių pavidalu, nes jie visada turi pranašumą virtualioje erdvėje. Taigi galima daryti išvadą, kad kuriama nauja kibernetinio saugumo koncepcija, kurioje prevencija sudaro didelę dalį. Autorių teigimu, kibernetinė erdvė kelia vis didesnę saugumo riziką ir iššūkį. Be to, kibernetinis saugumas reikšmingai paveiks XXI amžiaus tarptautinius santykius, o grėsmės ir iššūkiai didės.

2.2 Finansiniai kibernetinio saugumo iššūkiai

Leidinyje "Research report. Cybersecurity Technology Efficacy" (2020) rašoma, kad kibernetinis saugumas žlunga, nes technologijos nėra tokios efektyvios, kokios turi būti. Ši nuomonė pagrindžiama tuo, kad išlaidos kibernetiniam saugumui kasmet didėja (+58% per pastaruosius penkerius metus), tačiau, kaip kibernetinės atakos vis dar įvardijamos kaip vienos iš 5 didžiausių augančių rizikų 2020 m. (ir, nors tikslus skaičius yra ginčytinas, kryptis aiški). Pagrindinė šios nesėkmės priežastis yra ta, kad technologija nėra tokia efektyvi, kokia turi būti, ir tai 90 proc. atliktų mokslinių tyrimų išvadas aprašytas leidinyje. Nors pastaraisiais metais didelis dėmesys buvo skiriamas žmonių tobulinimui ir su procesu susijusiems klausimams, kurie, be abejo, prisideda ir prie kibernetinio saugumo trūkumų, technologinės problemos tam tikru būdu buvo pripažintos neišvengiamomis ir įprastos. Leidinyje perpasakojama kibernetinio saugumo eksperto nuomonė, „mes perkame (technologijas), tada sukryžiuojame pirštus ir tikimės, kad technologija veiks". Pasitikėjimas kibernetinio saugumo technologijomis, kad įvykdytų savo pažadą, yra menkas. Nepagerinus technologijų efektyvumo, kibernetinis saugumas ir toliau žlugs, štai tokia išvada pateikiama Debate security leidinyje.

Kibernetinis nusikalstamumas ir kibernetinis saugumas tapo viena svarbiausių temų. Remiantis įvairiais tyrimais, kibernetinis saugumas kelia didžiulį nerimą, o šalys, kurios neinvestuoja, nepaiso nerimą keliančių grėsmių ir (arba) neatsako laiku į kibernetines atakas, patiria didžiulius nuostolius. Kibernetinio saugumo problemos – ne tik įstatymų ar technologijų spragos. Kalbant apie kibernetinio saugumo planų įgyvendinimą, reikėtų paminėti, jog svarbus šio sektoriaus finansavimas.

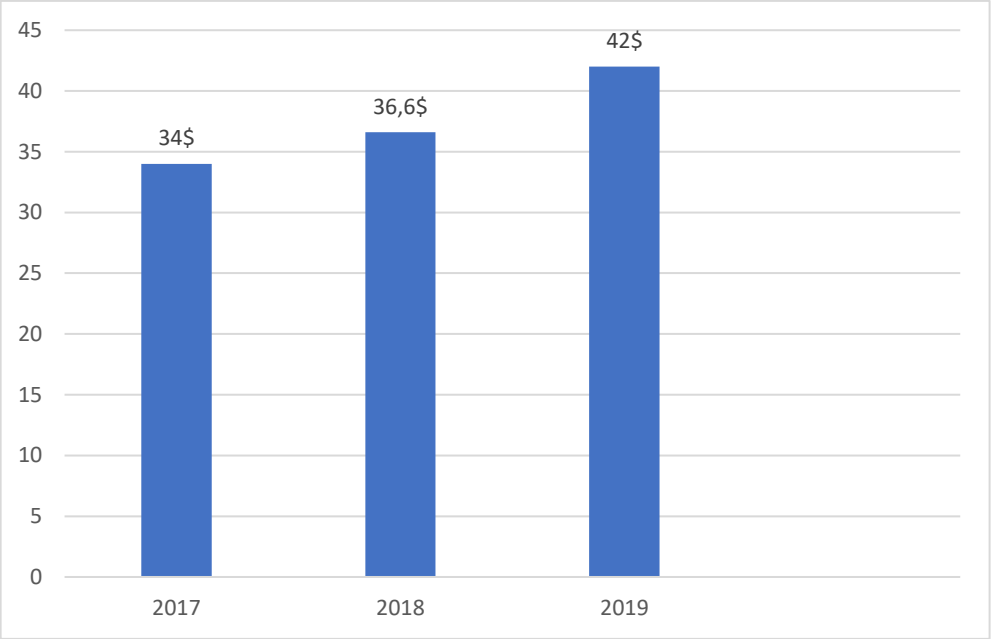
Svarbu suprasti skirtingų tipų investavimo strategijas, organizacinius veiksnius, turinčius įtakos sprendimų priėmimui ir derinimui bei individualiomis perspektyvomis dėl kibernetinio saugumo investicijų. Didelių duomenų apie investicijas, finansinę situaciją ir organizacinius kibernetinio saugumo veiksnius nėra. Literatūroje galima rasti investavimo strategijų, patarimų, kad investicijos kaina į

kibernetinį saugumą turėtų būti mažesnė už lyginamąją naudą, o investicija turėtų būti pagrįsta išsamiu kibernetinės rizikos vertinimu. Tyrėjai siūlo ekonominius modelius, pagal kuriuos nustatoma optimali investicijų suma. Rezultate - nedaugelis organizacijų nustato savo investavimo strategijas, remdamosi išsamia ekonominės naudos analize. Užuot tyrę optimalų investicijų lygį ar bandę tobulinti saugumo priemonių sąnaudas ir naudą įvertinančius modelius ar metodus, visų pirma reikia atsižvelgti į organizacinius veiksnius, kurie daro įtaką šioms strategijoms, ir asmenines perspektyvas, turinčias įtakos investavimo strategijoms.

B. Rowe ir M. P. Gallaheris (2006) atliko tyrimą, kuriuo siekė nustatyti sprendimų dėl kibernetinio saugumo investicijų priėmimo procesą. Jie daugiausia dėmesio skyrė į vidinės ir išorinės informacijos, kuri naudojama šiame sprendimų priėmimo procese, tipui. Autoriai svarsto dviejų tipų strategijas: aktyvią ir reaktyvią. Aktyvus pabrėžia prevenciją, o reaguoja reaguodamas į žinomas grėsmes. Vis dėl to yra skirtingų strategijų ir veiksnių, darančių įtaką šioms strategijoms. Tačiau vis dar reikia atlikti daugiau tyrimų apie sprendimų priėmėjų vaidmenį įmonėse, taigi, kas priima sprendimus? O kiek investavimo strategija daro įtaką realiam įgyvendinimui, o kas kuria įgyvendinimo strategiją ir ar šis asmuo taip pat gali daryti įtaką investavimo strategijai?

Kiek valstybei reikia investuoti - atsižvelgiant į finansus, laiką, žmogiškuosius išteklius - norint suteikti tinkamą kibernetinį saugumą? Biudžeto sudarymas kibernetiniam saugumui yra sudėtingas procesas, iš dalies todėl, kad saugumo priemonių įgyvendinimas nėra baigtinė užduotis: tai yra daugybė tarpusavyje susijusių, vykstančių procesų. Valstybės turi įtraukti saugumo aspektus ir testavimą į visą sistemų kūrimo, įsigijimo, diegimo, priežiūros ir palaikymo gyvavimo ciklą.

Siekdami sėkmingai suprasti kibernetinio saugumo poreikius ir numatyti jiems biudžetą, valstybės, įstatymų kūrėjai bei leidėjai turi suprasti kibernetinę terminologiją, suprasti kibernetinio saugumo riziką ir plėsti žinias apie tai, kokia veikla ir ištekliai gali padėti suplanuoti, reaguoti ir atsigauti po kibernetinių atakų, kai jos įvyksta. Šalys turi suprasti, kad pasirengimas yra nuolatinis procesas, kuriam reikalingas biudžetas, siekiant pašalinti kylančius iššūkius ir grėsmes. Įstatymų leidėjai turi apsvarstyti, kaip organizuojamos kibernetinio saugumo funkcijos ir kas kiekvienoje valstybėje yra atsakingas už kibernetinį saugumą. Šios žinios tiesiogiai paveiks nustatytinų valdymo, organizacinių ir finansavimo modelių tipą, mastą ir sudėtingumą (McSpaden, Appeaning, 2017).

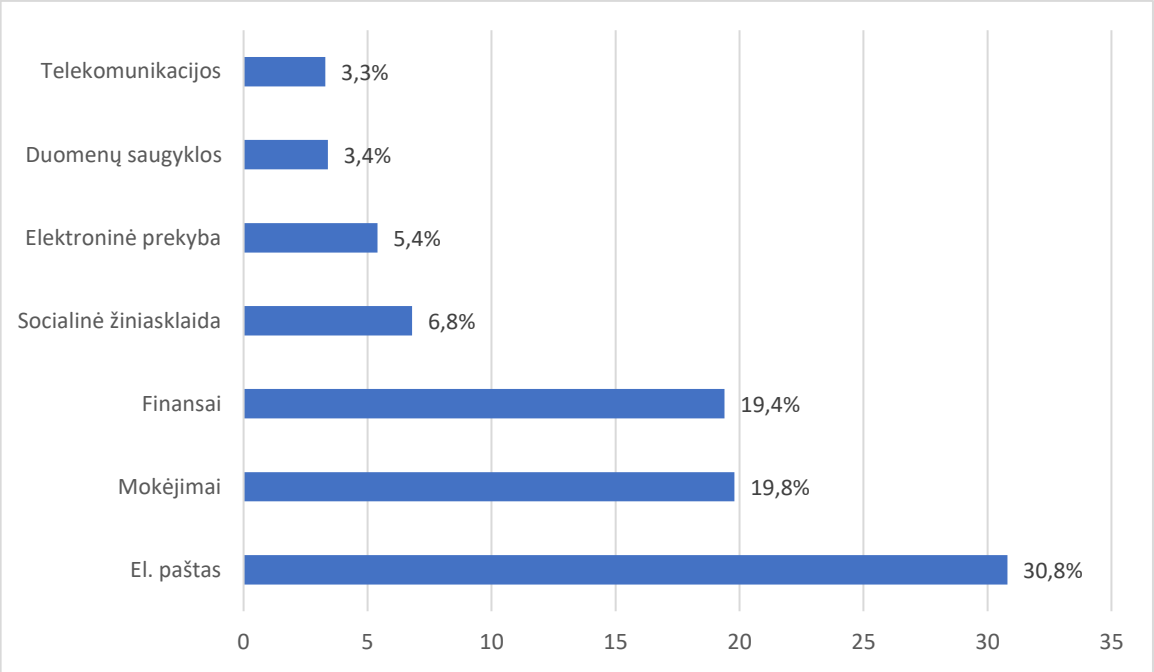


7 pav. Pasaulinės kibernetinio saugumo išlaidos (milijardais JAV dolerių)

Šaltinis: www.statista, 2020

7 pav. pavaizduota statistika rodo pasaulines išlaidas kibernetiniam saugumui nuo 2017 iki 2020 m. Nuo 2018 m. Išlaidos kibernetinio saugumo pramonėje siekė apie 37 milijardus JAV dolerių, o prognozės rodo, kad 2020 m. rinkoje užtikrinant kibernetinį saugumą atsiras 42 milijardai.

Statistika rodo, kad per paskutinįjį 2019 m. ketvirtį 19,4 proc. išpuolių visame pasaulyje buvo nukreipta į finansų įstaigas, net 30,8 proc. - internetinio pašto paslaugos. J. Vries (2017) teigimu, sprendimai dėl investicijų turėtų būti priimami remiantis išsamia ekonominės naudos analize ir kibernetinės rizikos vertinimu. Tačiau daugelis organizacijų neatlieka šios sudėtingos analizės, nes trūksta duomenų apie išlaidas, naudą ir išpuolių poveikį bei tikimybę. Svarbu siekti geriau suprasti šio sprendimo priėmimo procesą ir tai, kaip organizaciniai veiksniai ir individualios perspektyvos daro įtaką šiam procesui. J. Vries (2017) atliko tyrimą siekiant išsiaiškinti investavimo strategijas ir organizacinius veiksnius, kurie daro įtaką. Buvo nustatytos keturios skirtingos investavimo strategijos, kurios daugiausia skiriasi pradinėmis investicijomis ir pokyčiais per ateinančius dvylika mėnesių. Organizaciniai veiksniai, darantys įtaką šioms investavimo strategijoms, yra dydis, pajamos, tipas (viešasis / privatusis) ir biudžetas bei kiti veiksniai, tokie kaip reguliavimas, vadovybės supratimas, įvykiai ir rizikos rūšis.



8 pav. Sritys, kurios 2019 m. paskutinį ketvirtį labiausiai nukentėjo nuo kibernetinių atakų

Šaltinis: www.statista, 2020

2011 m. balandžio mėn. įvyko vienas didžiausių duomenų pažeidimų įmonės istorijoje. „Sony“ tai kainavo iki dviejų milijardų dolerių. „Sony“ nėra vienintelė įmonė, kurią užklupo kibernetinės atakos. Ir tai tik vienas iš pavyzdžių, kokių nuostolių gali patirti įmonė, organizacija ar vyriausybė. J. Vries (2017) teigimu vienas iš penkių ar vienas iš dešimties kompiuterių yra užkrėstas kokia nors kenkėjiška programa ir dažnai savininkui to nežinant. Augant kibernetinių atakų skaičiui, organizacijos gali patirti rimtų nuostolių ir turi apsvarstyti galimybę investuoti į savo saugumą, kiek jos turėtų investuoti ir kokias priemones įgyvendinti. Organizacijų, kurioms įtakos gali turėti kibernetinės atakos, vadovų informuotumas apie jų kibernetinį saugumą padidėjo, nes kibernetinės atakos įmonėms paprastai kainuoja milijonus. Tai leidžia organizacijoms geriau suvokti kibernetinę riziką, su kuria jos susiduria, ir reaguodamos į tai, organizacijos tobulina savo gynybą. Tačiau praktika rodo labai sunku nustatyti nuolat besikeičiančią kibernetinę riziką ir nustatyti, nuo ko reikia saugotis (Berg ir kt., 2014). Organizacijoms dažnai nėra aišku, kokios investicijos yra veiksmingos ir kokios investicijos suteikia „pakankamą apsaugą“ (Bojanc, Jerman-Blazic, 2008). Daugelis nerimauja dėl to, kad neturi pakankamai biudžeto, reikiamos komandos, reikiamų žinių, naujausių technologijų.

Racionalus požiūris į tinkamo saugumo lygio nustatymą apima visos rizikos, pažeidžiamumo, išpuolių tikimybės ir visų galimų išlaidų pažeidžiamumui sušvelninti nustatymą (Dynes, Goetz ir Freeman, 2008). Tuomet vienas didžiausių iššūkių yra apsvarstyti, kaip apsisaugoti nuo galimų kibernetinių išpuolių

ir kaip geriausiai panaudoti išteklius. Sprendimai dėl investicijų turėtų būti priimami remiantis išsamia ekonominės naudos analize, remiantis išpuoliais ir incidentais, dėl kurių organizacijos patiria didžiausią piniginės vertės praradimą. Tačiau daugelis organizacijų neatlieka šios sudėtingos finansinės analizės, nes trūksta duomenų apie išlaidas, naudą ir išpuolių tikimybę (Rowe ir Gallaher, 2006). Taigi retai kada organizacija, prieš priimdama sprendimą dėl investavimo, atlieka išsamią išlaidų ir naudos analizę ar kibernetinės rizikos vertinimą. Tačiau kaip šalys nustato, kiek jos turėtų išleisti kibernetiniam saugumui?

- Kas skatina kibernetinio saugumo investicijas?
- Kokios kibernetinio saugumo investavimo strategijos egzistuoja praktikoje?
- Kokie veiksniai daro įtaką kibernetinio saugumo investavimo strategijoms?
- Kokios yra individualios sprendimų priėmėjų perspektyvos dėl investicijų į kibernetinį saugumą strategijas?
- Ar šias investavimo strategijas galima paaiškinti iš sprendimų priėmėjų perspektyvos?

Kiekviena organizacija ir vyriausybė turi žinoti, kiek reikia investuoti į kibernetinį saugumą. P. Brangetto bei M. Kert-Saint Aubyn (2015) teigimu, reikia pastebėti, kad mažai dėmesio skiriama kibernetinio saugumo ekonomikai, kuri pateikia keletą įdomių ir tinkamų modelių, skirtų įvertinti kibernetinio saugumo investicijas, atliekant išlaidų ir naudos kompromisus. Autoriai pateikia išvadas, pagrįstas nacionalinių kibernetinio saugumo strategijų analize, kuriomis siekiama bandyti įvertinti pagrindinius ekonominius elementus rengiant ir priimant nacionalines kibernetinio saugumo strategijas visame pasaulyje.

Brangetto bei M. Kert-Saint Aubyn (2015) darbe "Nocionalinių kibernetinių saugumo strategijų ekonominiai aspektai" aprašo kibernetinio saugumo ekonomikos būklę. Autorių tikslas buvo nustatyti, kiek nacionalinėse kibernetinio saugumo strategijose buvo atsižvelgta į ekonomikos principus ir kiek turimos priemonės yra tinkamos rengiant strategijas. Autoriai pateikia kibernetinio saugumo ekonomikos analizę ir pateikia informaciją, kiek valstybės ėmėsi šių principų ir juos pritaikė savo nacionalinėse kibernetinio saugumo strategijose.

Klausimas, kaip įvertinti kibernetinio saugumo efektyvumą, vis dar yra neatsakytas. Buvo daug bandymų užtikrinti investicijų grąžos pagrindą saugumui - procesas, kuris dažnai žlunga, nes sunku apskaičiuoti pelną. Vienas iš pagrindinių tikslų, kurių siekiama užtikrinant kibernetinę erdvę, yra šalies galimybė išlaikyti savo ekonominę veiklą naudojantis informacinėmis ir ryšių technologijomis (IKT).

Manoma, kad labai svarbu, kad veikla, vykdoma elektroninėmis priemonėmis (bankininkystė, mažmeninė prekyba, įvairios paslaugos, administravimas ir kt.) būtų apsaugota.

Kalbant apie ES reikia paminėti, jog ES siekia tapti saugiausia kibernetinio saugumo zona. Šiam užmojui pasiekti reikia didelių visų suinteresuotųjų šalių pastangų, įskaitant finansinį pagrindą ir su tuo susijusį investicijų didinimą. Leidinyje "Veiksmingos ES kibernetinio saugumo politikos iššūkiai" (2019) rašoma, jog apskaičiuota, kad visos pasaulinės kibernetinio saugumo išlaidos, išreikštos BVP procentine dalimi, bus apie 0,1%. Jungtinėse Valstijose šis skaičius padidėjo iki maždaug 0,35% (įskaitant privatųjį sektorių). Kalbant apie BVP procentą, JAV federalinės vyriausybės išlaidos sudaro apie 0,1% arba 21 milijardą JAV dolerių. ES išlaidos palyginti yra nedidelės, fragmentiškos. Skaičius sunku apskaičiuoti, tačiau manoma, kad ES išlaidos kibernetiniam saugumui svyruoja nuo vieno iki dviejų milijardų eurų per metus. Kai kurių valstybių narių išlaidos procentais nuo BVP yra viena dešimtoji JAV lygio arba net mažesnės.

Dėl sudėtingo kibernetinio saugumo pobūdžio ir dėl to, kad kibernetinis saugumas ir bendros IT išlaidos dažnai nesiskiria, sunku sudaryti išsamų vaizdą, nes nėra aiškių duomenų. Autorių nuomone, sunku gauti patikimą statistiką apie išlaidas tiek viešajame, tiek privačiame sektoriuose. Trys ketvirtadaliai nacionalinių audito biurų teigė neturintys centralizuotos su kibernetinėmis vyriausybėmis susijusių išlaidų apžvalgos. Didinti viešojo ir privačiojo sektoriaus investicijas Europos kibernetinio saugumo įstaigose yra didelis iššūkis. Yra daugybė ES finansavimo iniciatyvų, tačiau jomis nesinaudojama, daugiausia dėl biurokratijos. Norint pasiekti ES skaitmeninės politikos tikslus labai svarbu užtikrinti veiksmingą finansavimą.

Dėl daugelio aspektų sunku nustatyti optimalų saugumo ir investicijų lygį. Pirma, yra ribotas patikimos informacijos, o antra, sunku nustatyti riziką, su kuria susiduriama, ir nustatyti tikrąjį rizikos, atsirandančios dėl įvairių grėsmių ir besikeičiančios aplinkos, poveikį ir tikimybę. Kaip žmonės galvoja apie riziką, labai svarbu geriau suprasti šį procesą. Ir paskutinis dalykas yra tai, kad žmonės ne visada priima geriausius sprendimus. Bet koks sprendimas dėl kibernetinio saugumo visada susijęs su savotišku kompromisu, nesvarbu, ar tai išlaidos, laikas, patogumas, ištekliai, galimybės ir pan. Be to, žmonės gali būti linkę į įvairius šališkumus priimant sprendimus (Kahneman, 2011).

Siekdamos kažkaip priimti sudėtingus sprendimus susijusius su investicijomis į kibernetinį saugumą, daugelis organizacijų supranta didėjančią rizikos valdymo svarbą. Galima teigti, kad rizikos valdymas yra pats sprendimų priėmimo procesas. Vienaip ar kitaip, yra įvairių rizikos valdymo procesų, plačiai naudojamų organizacijose, o vieni iš jų geresni nei kiti. Norint valdyti riziką, reikia suprasti riziką. Todėl galima naudoti rizikos valdymą, tai yra rizikos nustatymo, apibūdinimo ir supratimo procesas (Soo

Hoo, 2000). Standartiniame rizikos vertinime siūloma riziką suskirstyti į dvi sudedamąsias dalis: 1) rizikos atsiradimo tikimybę ir 2) poveikį, kurį rizika gali sukelti, tada padauginus išmatuoti rizikos dydį. Tačiau šis pagrindinis metodas gali būti nepraktiškas ir neracionalus, kai taikomas aklai, todėl jo ne visada pakanka priimant sprendimus (Neil, 2012). Labiau struktūruotas procesas yra NEN-ISO 31000 atliekamas vertinimas, kurį sudaro šie penki etapai: konteksto nustatymas, rizikos nustatymas, rizikos analizė, rizikos vertinimas ir rizikos šalinimas. Tai atrodo labai skaidrus ir objektyvus procesas, tačiau sprendimai dėl kibernetinio saugumo priimami remiantis subjektyviais sprendimais. Be to, atliekant šį kibernetinės rizikos vertinimą sprendimai priimami paprastai neturint informacijos apie pasekmių tikimybes, įvykių tikimybę (Vries, 2017). Taigi galima teigti, kad tai yra sprendimų priėmimas netikrumo dėka. Tačiau taip pat galima teigti, kad rizika iš prigimties yra neapibrėžta, o jai pašalinti naudojama rizikos valdymas.

Taigi kur yra sprendimai, priimami rizikos valdymo metu? Kibernetinės rizikos valdymo procesas yra sudėtingas. Valdant ir vertinant kibernetinę riziką, priimami keli sprendimai. Galima daryti išvadą, kad šiam sprendimui gali turėti įtakos visas kibernetinės rizikos valdymo sprendimų procesas, tačiau organizacijos taip pat galėtų sutelkti dėmesį tik į nedidelę rizikos valdymo dalį, taigi tik ši maža dalis daro įtaką investavimo strategijai.

Lieka klausimas: ar kiekviena organizacija atlieka tokį išsamų rizikos vertinimą? Teoriškai rizikos vertinimas yra naudojamas norint paremti geriausią sprendimą, tačiau ar jis veikia ir yra naudojamas praktikoje? Pavyzdžiui, ar organizacijos biudžetas lemia, kokiu mastu atliekamas rizikos vertinimas? Jei taip, ar tai reiškia, kad mažesnės organizacijos priima sprendimus, nepagrįstus rizikos vertinimu? Tai, kaip asmuo naudoja rizikos vertinimą, gali būti perspektyva, kurią profesionalas priima priimant sprendimus. Taigi, pavyzdžiui, asmuo kreipia dėmesį tik į kibernetinę riziką ir atsižvelgia tik į vieną rizikos rūšį: nerūpestingo darbuotojo riziką. Tuomet šis asmuo imasi tik priemonių šiai rizikai valdyti ir nustato savo investavimo strategiją tik remdamasis šia rizika.

3. KIBERNETINIO SAUGUMO ĮGYVENDINIMO YPATUMŲ VERTINIMAS

3.1 Tyrimo metodologija

Šiuo empiriniu tyrimu siekiama išanalizuoti kibernetinio saugumo ekspertų patirtis. Siekiant atskleisti ekspertų, dirbančių kibernetinio saugumo srityje patirtis, pasirinktas **kokybinis tyrimo metodas**. Kokybinio tyrimo tikslas – tyrinėti tam tikrus reiškinius ir tiriamųjų požiūrius apie tiriamą reiškinį (Bitinas, 2013). Tyrime taikytas pusiau struktūrizuotas interviu metodas, kuris leidžia priartėti prie informantų patirčių suvokimo (Kardelis, 2002).

Tyrimo objektas – kibernetinio saugumo kaštų tendencijos.

Tyrimo tikslas – Išanalizuoti kibernetinio saugumo kaštų tendencijas Lietuvoje ir pasaulyje.

Darbo uždaviniai:

1. Atskleisti kibernetinio saugumo sampratą;
2. Išanalizuoti transnacionalinio kibernetinio saugumo padėtį;
3. Atlikti kibernetinio saugumo ekspertų interviu siekiant atskleisti kibernetinio saugumo ir kaštų koreliacijas.

Tyrimo dalyviai: Ekspertai, dirbantys kibernetinio saugumo srityje. Pagrindiniai reikalavimai ekspertams: IT srities aukštasis išsilavinimas; turėti ne mažesnę nei 5 metų darbo patirtį užtikrinant organizacijoje informacijos saugą (kibernetinis saugumas). Ekspertai pasižymintys geras rizikos valdymo principų ir priemonių, organizacijos veiklos procesų ir bendrųjų teisės aktų išmanymu; geru kibernetinę saugą reglamentuojančių teisės aktų išmanymu; analitiniu mąstymu, įžvalga, gebėjimu taikyti teisės aktus; elektroninės informacijos išmanymu ir kibernetinio saugumo užtikrinimo principų ir teisės aktų bei standartų, reglamentuojančių elektroninės informacijos saugą ir kibernetinį saugumą, reikalavimus ir saugos užtikrinimo gerąją praktiką.

Imties sudarymo būdas. Sudarant tyrimo imtį, bus naudojamas netikimybinės atrankos būdas – tikslinė atranka. Į apklausiamą grupę įtraukiant pačius tipiškiausius bei informatyviausius asmenis tiriamojo požymio atžvilgiu. Todėl šiame tyrime imties tipas bus tikslinė imtis, tai yra ekspertai, dirbantys kibernetinio saugumo srityje.

Ginamieji teiginiai:

1. Kibernetinio saugumo finansavimo trūkumas lemia kibernetines problemas Lietuvoje.
2. Siekiant kibernetinio saugumo efektyvumo svarbu didinti finansavimą.

Tyrimo ribotumas:

• tyrėjo asmeninė patirtis ir žinios gali daryti įtaką pastebėjimams ir išvadoms;

• dėl tyrimo atvirumo tiriamieji gali kontroliuoti duomenų gavimą (surinkimą) ir duomenų rezultatai negali būti patikrinti objektyviai (Bitinas, 2013; Kardelis, 2002).

Siekiant įvertinti ekspertų, dirbančių kibernetinio saugumo srityje patirtis buvo atliktas tyrimas. Informantams pateikti 11 klausimų (priedas nr. 1). Tyrimo metu gauti duomenys analizuojami taikant turinio (content) analizę. Interviu analizė išskaidyta į 3 dalis:

1. duomenų skaitymas;
2. kategorijų ir subkategorijų išskyrimas;
3. analizė ir interpretacija.

Tyrimo imtis. Tyrime naudota tikslinė kriterinė imtis. Informantai parinkti pagal tam tikrus kriterijus: ekspertai dirbantys kibernetinio saugumo srityje. Tyrime dalyvaujantiems ekspertams suteikti vardai: informantas 1 (I 1), informantas 2 (I 2), informantas 3 (I 3), informantas 4 (I 4), informantas 5 (I 5), informantas 6 (I 6), informantas 7 (I 7), informantas 8 (I 8). Organizuojant tyrimą nebuvo numatytas tikslus informantų skaičius. Iš anksto buvo nuspręsta atlikti interviu kol duomenys pradės kartotis ar/ir taps panašūs. Anot Bitino (2013), tik tuomet kai tyrėjas supranta, jog situacija kartojasi, jis gali nutraukti tyrimą. Pastebėjus, kad tyrimo metu interviu buvo atlikta su aštuoniais informantais t.y. lyginis skaičius buvo svarstoma galimybė atlikti ekspertinį kriterijų vertinimą remiantis prielaida, kad tyrimų rezultatai gali būti gauti tik įvertinus ekspertų nuomonių suderinamumą. Vienas iš dažniausiai naudojamų koeficientų, leidžiančių įvertinti dalyvavusių ekspertų nuomonių suderinamumą, yra Kendall konkordancijos koeficientas W. Jei ekspertų vertinimai prieštaringi konkordancijos koeficiento reikšmė W artėja prie 0, jei ekspertų vertinimai panašūs - W artėja prie 1. Kai visos ranguotės sutampa, tokiu atveju W = 1.

Bet atskleidus , kad ekspertų interviu metodas taikomas , iki tol kol informacija pradeda kartotis, tada sustojama daryti interviu, visiškai nesvarbu kiek interviu iki tol buvo padaryti. Tai vadinama tyrimo prisotinimu. Buvo padaryta išvada , kad šiam tyrimo metodui netikslinga taikyti ekspertų nuomonių suderinamumo skaičiavimus.

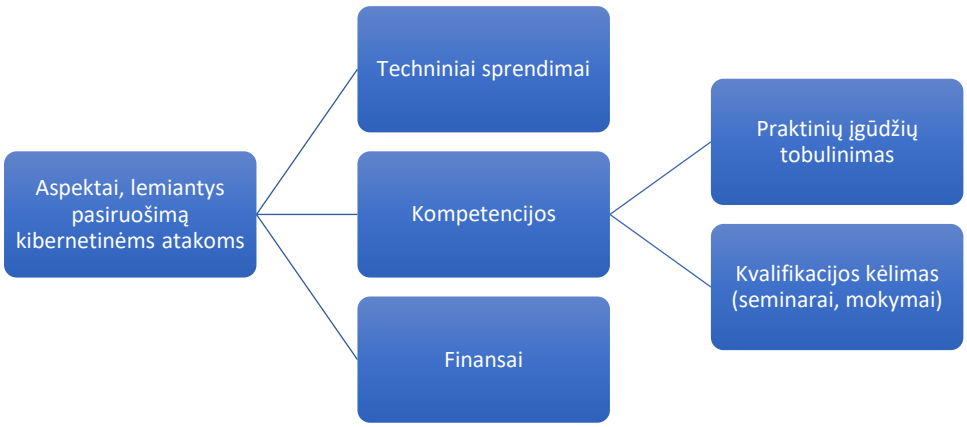
Tyrimo organizavimas: Atliekant tyrimą visi informantų pasisakymai su jų sutikimu buvo įrašomi. Atlikus interviu, informantų atsakymai perrašomi į tekstą. Tyrimas atliktas 2020 spalio 1-31 dienomis. Pusiau struktūruotas interviu truko nuo 20 min. iki 45 min.

Tyrimo etika. Tyrimo pradžioje su informantais buvo aptartas konfidencialumo klausimas, t. y. bus saugomas dalyvių bei tyrimo duomenų anonimiškumas, kuris neleis nustatyti informantų tapatybės. Tyrimas atliktas laikantis informavimo principo, prieš tyrimą buvo pateikta išsami informacija apie planuojamą vykdyti tyrimą. Prieš atliekant tyrimą informantams buvo paaiškinta, kur ir kaip bus naudojama informacija, kuri bus gauta tyrimo metu, pateikta visa informacija apie galimą darbo naudą mokslui ir tyrimo dalyviams, atsakyta į tyrimo dalyvių kilusius klausimus. Buvo išlaikytas savanoriško dalyvavimo tyrime principas (Kardelis, 2002).

Tyrimo duomenų analizė. Tyrimo duomenis apdoroti taikomas turinio (content) analizės metodas. Analizuojant interviu taikoma kodavimo procedūra pagal raktinius žodžius išskiriant kategorijas ir subkategorijas. Tyrimo duomenys pavaizduoti paveiksluose, kuriuose pateikiamos išskirtos kategorijos ir subkategorijos. Kategorijas ir subkategorijas iliustruoja teiginiai iš informantų interviu.

3.2 Tyrimo duomenų analizė

Tyrimu taip pat siekta išsiaiškinti, kokie ***pagrindiniai aspektai lemiantys pasiruošimą kibernetinėms atakoms*** (9 pav.).



9 pav. Aspektai, lemiantys pasiruošimą kibernetinėms atakoms

Analizuojant tyrimo duomenis išskirtos trys grupės aspektų darančių įtaką kibernetiniam saugumui. Tyrimo duomenų analizė atskleidė 3 subkategorijos: ***techniniai sprendimai, kompetencijos, finansai***. Interviu atskleidė, jog ***techniniai*** valstybės, didelių, vidutinių ir mažų įmonių ***sprendimai*** nulemia kibernetinių atakų sėkmę:

techniniai sprendimai: *„<...> Pasiruošimas priklauso ne tik nuo techninių ir organizacinių bet ir nuo žmogiško faktoriaus. Apsisaugoti nuo kibernetinių atakų galime tik apjungus technines ir organizacines priemones <...>.“* (I 6)

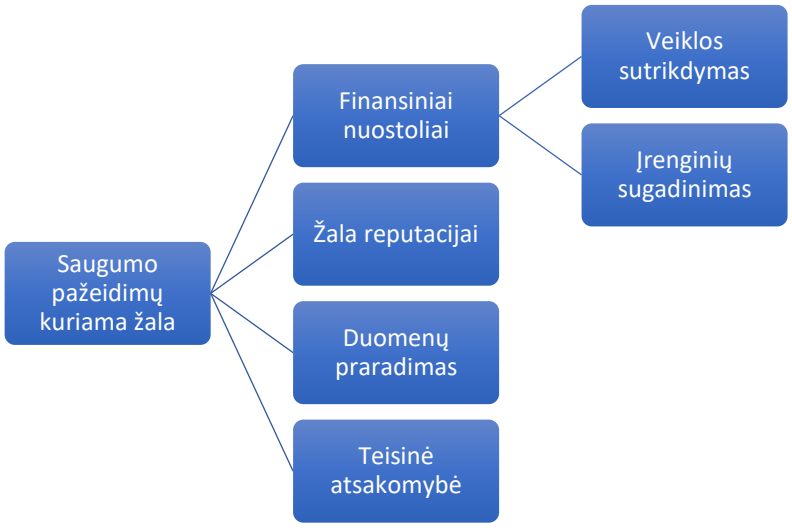
Dar vienas aspektas, kurį išskyrė ekspertai – ***kompetencijos***. Interviu duomenų analizė atskleidė, jog informantų nuomone, praktinių įgūdžių tobulinimas bei kvalifikacijos kėlimas, nuolatinis žinių atnaujinimas taip pat prisideda prie sėkmingų kibernetinių atakų baigčių:

kompetencijos: *„<...> organizuojamos įvairių įstaigų pratybos nacionaliniu mastu „Kibernetinis skydas 2019“ <...>.“* (I 5)
„<...> Reikalingas didelis dėmėsis vartotojų kibernetinio saugumo mokymams <...>.“ (I 6)
„<...> Kalbant apie valstybę dažniausiai testuojant saugumą, reikalaujama ir bandoma į jas įsilaužti, kad atrasti tas spragas per kurias galima įsilaužti <...>.“ (I 8)

Dar vienas populiarus aspektas – ***finansai***. Ekspertai dalyvavę tyrime atskleidė, jog finansavimo klausimas ypač aktualus ir svarbus kalbant apie kibernetinį saugumą. Būtent finansai susiję su technine kibernetinio saugumo dalimi, galimybę kelti kompetenciją šioje srityje bei apmokėti kibernetinio saugumo ekspertui už jo darbą:

finansai: *„<...> Didžiosios įmonės įsivertinusios kibernetinių atakų pasekmes investuoja į kibernetinį saugumą <...>.“* (I 2)
„<...> naudojamos nemažos lėšos, kas yra gerai <...>.“ (I 5)

Tyrimo metu siekta išsiaiškinti aspektus, lemiančius pasiruošimą kibernetinėms atakoms, tačiau ir tai, kokia ***žala patiriama dėl saugumo pažeidimų*** (10 pav.).



10 pav. Saugumo pažeidimų kuriama žala

Analizuojant tyrimo duomenis išskirtos keturios sritys, kurioms saugumo pažeidimai daro žalą. Tyrimo duomenų analizė atskleidė 4 subkategorijos: ***finansiniai nuostoliai, žala reputacijai, duomenų praradimas, teisinė atsakomybė***. Kalbant apie saugumo pažeidimų atnešamus ***finansinius nuostolius*** ekspertai pabrėžė, jog tai gali būti susiję tiek su veiklos sutrikdymu, tiek su įrenginių sugadinimu, teisinė atsakomybė taip pat gali atnešti finansinių nuostolių:

finansiniai nuostoliai: *„<...> duomenų (asmens duomenų) vagystės, subjektų veiklos sutrikdymas, ar net įrenginių sugadinimas <...>.“* (I 3)
„<...> Finansinė žala (pvz. norint atgauti užšifruotus duomenis tenka mokėti išpirką; kenkėjiškas programinės įrangos sutrikdyta įmonės veikla lemia negautas pajamas, pagal suklastotą laišką atliktas pavedimas į sukčių sąskaitą ir pan.) <...>.“ (I 7)

Antras aspektas, kurį išskyrė ekspertai – ***žala reputacijai***. Interviu duomenų analizė atskleidė, jog informantų nuomone, žala reputacijai taip pat gali sietis su klientų nepasitikėjimu, pelno praradimu:

žala reputacijai: *„<...> pasitaiko atvejų kai saugumo pažeidimas gali diskriminuoti asmenį visuomenėje <...>.“* (I 2)

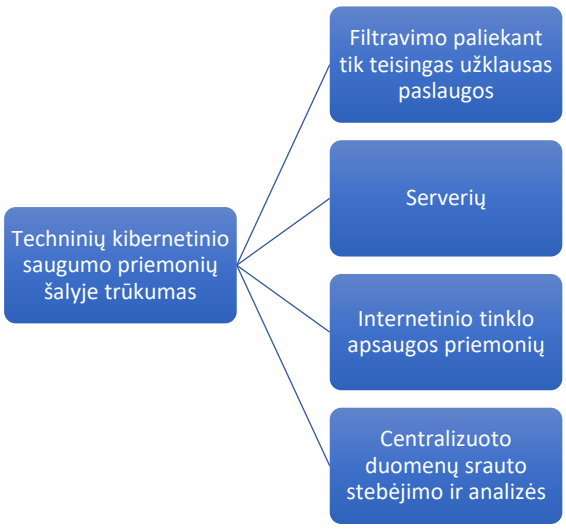
Dar vienas aspektas – ***duomenų praradimas***. Ekspertai dalyvavę tyrime atskleidė, jog duomenų praradimas gali būti siejamas taip pat su finansiniais nuostoliais, teisine atsakomybę, o medijų aprašyti įvykiai kenkia reputacijai (klientų praradimas, nepasitikėjimas):

duomenų praradimas: *„<...> intelektualinės nuosavybės praradimas (pvz. pavogta įmonės vykdomų mokslinių tyrimų, kuriamų inovatyvių produktų informacija) <...>.“* (I 7)

Ketvirtas aspektas, kurį išskyrė informantai interviu metu – ***teisinė atsakomybė***. Ekspertai pabrėžė, jog saugumo pažeidimų sukeliamas duomenų praradimas, netinkamas duomenų saugojimas gali sukelti teisinę atsakomybę:

teisinė atsakomybė: *„<...> teisinių pasekmių žala (“Grožio chirurgijos” atvejis, kai įmonės užsidarymą galimai lėmė pavogti klientų sveikatos duomenys ir gręsiantys ieškiniai) <...>.“* (I 7)

Tyrimu taip pat siekta išsiaiškinti, ekspertų nuomone, kokių techninių kibernetinio saugumo priemonių trūksta šalyje (11 pav.).



11 pav. Techninių kibernetinio saugumo priemonių trūkumas šalyje

Tyrimo dalyviai interviu metu išskyrė keturias priemones, kurios gali padėti labiau užtikrinti kibernetinį saugumą. Tyrimo duomenų analizė leido išskirti 4 subkategorijos: ***filtravimo paliekant tik teisingas užklausas paslaugos, serverių, internetinio tinklo apsaugos priemonių, centralizuoto duomenų srauto stebėjimo ir analizės***. Viena iš priemonių padėsiančių labiau užtikrinti kibernetinį saugumą, ekspertų nuomone, filtravimo paliekant tik teisingas užklausas paslauga:

filtravimo paliekant tik teisingas užklausas paslauga: *„<...> Didelio duomenų srauto atakos atveju filtravimo paliekant tik teisingas užklausas paslaugos <...>.“* (I 2)

Dar vienas aspektas, kurį išskyrė ekspertai – ***serveriai***. Informantai pabrėžė, jog šią priemonę įtraukti į sąrašą paskatino įvykiai Registrų centre:

serveriai: *„<...> Kaip parodė šių metų praktika, Lietuvoje trūksta gerų serverių, iš kurių būtų nesunkiai atstatyti prarasta informaciją <...>.“* (I 8)

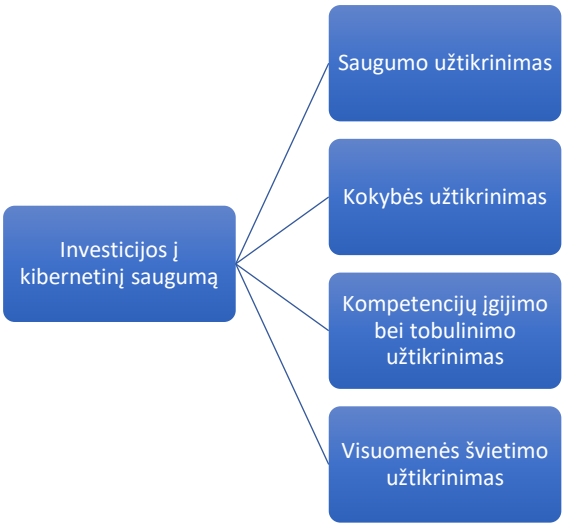
Trečia priemonė, kurią išskyrė informantai interviu metu – ***internetinio tinklo apsaugos priemonės***. Ekspertai įsitikinę, jog svarbu šviesti, kas tai yra ir kodėl ši priemonė yra svarbi:

internetinio tinklo apsaugos priemonės: *„<...> Internetinio tinklo apsaugos priemonių. Manyčiau, kad neužtenka vien internetinio tinklo paslaugų tiekėjus priskirti prie kritinės infrastruktūros, būtina jiems kelti atitinkamus reikalavimus ir nuolat vertinti jų įgyvendinimą <...>.“* (I 1)

Ketvirta ir paskutinė priemonė, kurią įvardino ekspertai – ***centralizuoto duomenų srauto stebėjimo ir analizės***. Ekspertai pabrėžė, jog bet kuriuo atveju svarbus bendradarbiavimas tiek tarp institucijų, tiek tarp ekspertų, patirčių ir praktikų pasidalijimas:

centralizuoto duomenų srauto stebėjimo ir analizės: *„<...> Daugiau centralizuoto duomenų srauto stebėjimo ir analizės <...>.“* (I 7)

Tyrimu taip pat siekta išsiaiškinti, ekspertų nuomone apie investicijas į kibernetinį saugumą (12 pav.).



12 pav. Investicijos į kibernetinį saugumą

Analizuojant tyrimo duomenis paaiškėjo, kodėl, ekspertų nuomone, svarbu investuoti į kibernetinį saugumą. Tyrimo duomenų analizė atskleidė 4 subkategorijas: ***saugumo užtikrinimas, kokybės užtikrinimas, kompetencijų įgijimo bei tobulinimo užtikrinimas ir visuomenės švietimo užtikrinimas***. Interviu atskleidė, jog investicijos gali padėti užtikrinti saugumą, skiriant finansus specialistams, ekspertams, priemonėms saugumui užtikrinti, sudarant sąlygas kelti kvalifikaciją bei tobulinti kompetencijas:

saugumo užtikrinimas: *„<...> Investicijos į kibernetinį saugumą užtikrina tolimesnę ateitį be neigiamų pasekmių <...>.“* (I 2)

„<...> kai technologijos sparčiai tobulėja, o specialistų daugėja, tokiu pačiu principu veikia ir kenkėjų skaičius, todėl investicija į kibernetinį saugumą yra privalu <...>.“ (I 8)

Dar vienas aspektas, kurį išskyrė ekspertai – ***kokybės užtikrinimas***. Informantai pabrėžė, jog investicijos leidžia užtikrinti kokybę kalbant tiek apie priemones, tiek apie investicijų keliamas galimybes:

kokybės užtikrinimas: *„<...>* pastoviai neinvestuojant kibernetinio saugumo kokybė blogėtų <...>.“ (I 5)

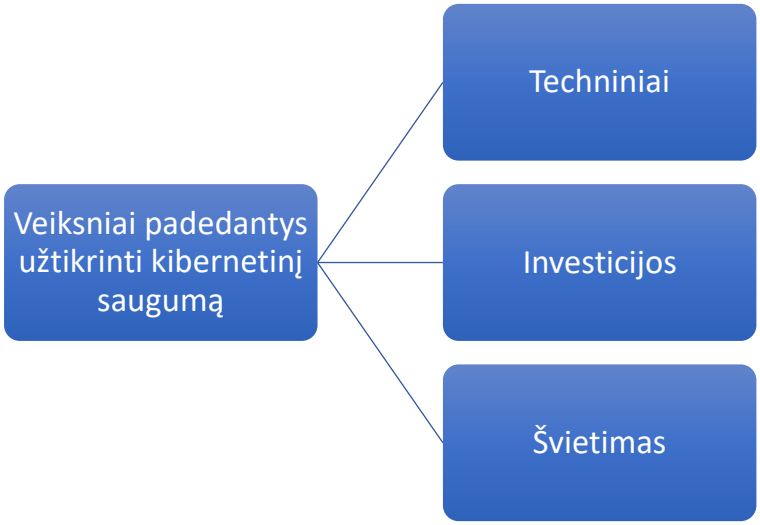
Trečias aspektas, kurį išskyrė informantai interviu metu ***kompetencijų įgijimo bei tobulino užtikrinimas***. Interviu dalyvavę ekspertai pabrėžė, jog investicijos leidžia kelti kompetenciją, tobulinti turimas žinias:

kompetencijų įgijimo bei tobulino užtikrinimas: *„<...> Manyčiau didžiausios investicijos turi būti nukreipiamos į kompetencijos centrų kūrimą (labai geras pvz. Estijoje įkurtas NATO kibernetinio saugumo centras)* <...>.“ (I 1)

Dar vienas aspektas, kurią įvardino ekspertai ***visuomenės švietimo užtikrinimas***. Ekspertai pabrėžė, jog bet kuriuo atveju svarbus visuomenės švietimo užtikrinimas. Būtent ši priemonė leistų mažinti galimybes kibernetiniam saugumui, duomenų vagystėms:

visuomenės švietimo užtikrinimas: *„<...> visuomenės įtraukimas į kibernetinio saugumo užtikrinimą* <...>.“ (I 1)
„<...> labai tikslingai investuojant į piliečių švietimą <...>.“ (I 3)

Analizuojant tyrimo duomenis išskirtos 3 subkategorijos veiksnių, padedančių užtikrinti kibernetinį saugumą (13 pav.).



13 pav. Veiksniai, padedantys užtikrinti kibernetinį saugumą

Analizuojant tyrimo duomenis buvo išskirtos 3 subkategorijos: ***techniniai sprendimai, investicijos ir švietimas:***

techniniai: *„<...> legali programinė įranga, atnaujinimai, gerųjų praktikų naudojimas, antivirusinė apsauga, tinklų ir potinklių tvarkingumas, atskyrimas, srautų valdymas, stebėjimas, naujų technologijų (tokių, kaip threat intelligence, prijungtų prie dirbtinio intelekto galingų sistemų, analizuojančių milžiniškus kiekius tinklo paketų)* <...>.“ (I 3)
„<...> Tinkamų ir apsaugotų su šifravimais svetainių naudojimas <...>.“ (I 8)

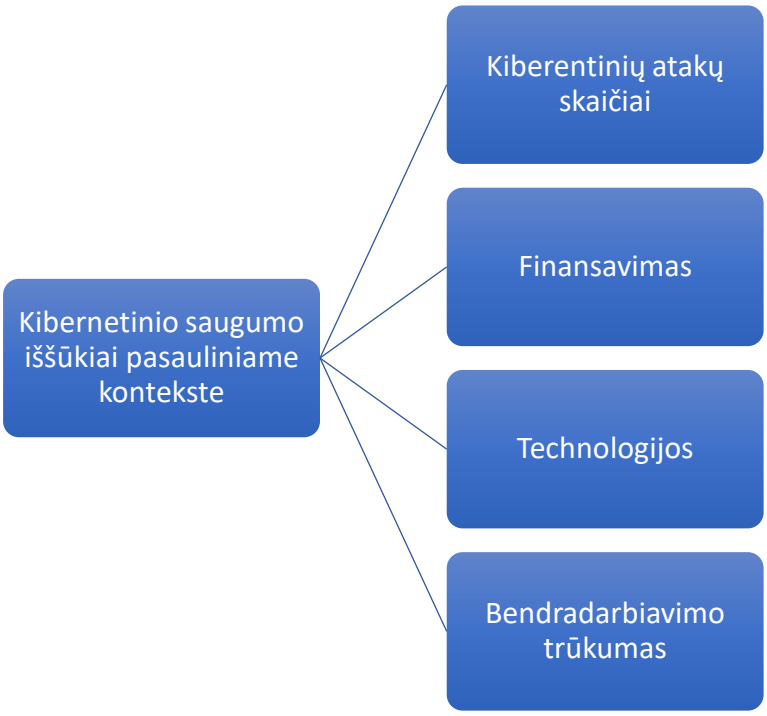
Dar vienas aspektas, kurį išskyrė ekspertai – ***investicijos***. Informantai pabrėžė, jog investicijos leidžia užtikrinti kokybę kalbant tiek apie priemones, tiek apie įrangą ar/ir personalą:

investicijos: *„<...> Įstaigų ar bendrovių vadovai turi aiškiai suprasti , kad tik investicijos į personalą (mokymai) ir į kibernetinio saugumo priemones, rizikų analizes gali ženkliai sumažinti pažeidžiamumą ir išpuolio pasekmes* <...>.“ (I 6)

Trečias aspektas, kurį išskyrė informantai interviu metu ***švietimas***. Interviu dalyvavę ekspertai pabrėžė, jog tiek darbuotojų, tiek nuolatinis visuomenės švietimas mažina kibernetinių atakų rizikas:

švietimas: *„<...> nuolatinis darbuotojų švietimas ir sąmoningumo ugdymas* <...>.“ (I 1)
„<...> Nuolatinis žmonių sąmoningumo ir kompetencijų lygio kėlimas kibernetinio saugumo srityje<...>.“ (I 4)
„<...> darbuotojų kompetencijos bei pastovūs mokymai <...>.“ (I 5)

Analizuojant tyrimo duomenis ekspertai išskyrė 4 subkategorijas – kibernetinio saugumo iššūkiai pasauliniame kontekste (14 pav.).



14 pav. Kibernetinio saugumo iššūkiai pasauliniame kontekste

Analizuojant tyrimo duomenis buvo išskirtos 4 subkategorijos: ***kibernetinių atakų skaičiai, finansavimas, technologijos, bendradarbiavimo trūkumas:***

kibernetinių atakų skaičiai: *„<...> Vis didėjantys kibernetinių atakų mastai <...>.“* (I 2)
„<...> Tinkamų ir apsaugotų su šifravimais svetainių naudojimas <...>.“ (I 8)

Antras aspektas, kurį išskyrė informantai interviu metu **- *finansavimas***. Interviu dalyvavę ekspertai pabrėžė, jog reiktų kalbėti apie įtakingas, turtingas šalis, kurios investuoja į šnipinėjimą, užsiima žvalgyba:

finansavimas: *„<...> Aktyvus nedraugiškų valstybių, turinčių didelius finansinius ir kitus resursus aktyvia žvalgybine veikla kibernetinėje erdvėje (niekada negali žinoti, kokias jie yra jau nustatę spragas ir kada bei kokiu mastu jas gali panaudoti) <...>.“* (I 1)
„<...> Mano nuomone, vieni didžiausių iššūkių kibernetinio saugumo srityje yra suinteresuotų valstybių (dažniausiai ne demokratinių, bet nebūtinai) milžiniškais finansiniais resursais aprūpintos kibernetinio šnipinėjimo ir sabotažo operacijos, darančios didelę įtaką geopolitikai (pastarieji JAV prezidento

rinkimai). Taip pat vis didėja grėsmė pamatinėms žmogaus teisėms į privatumą (Kinijos masinis žmonių sekimas) <...>.“ (I 4)

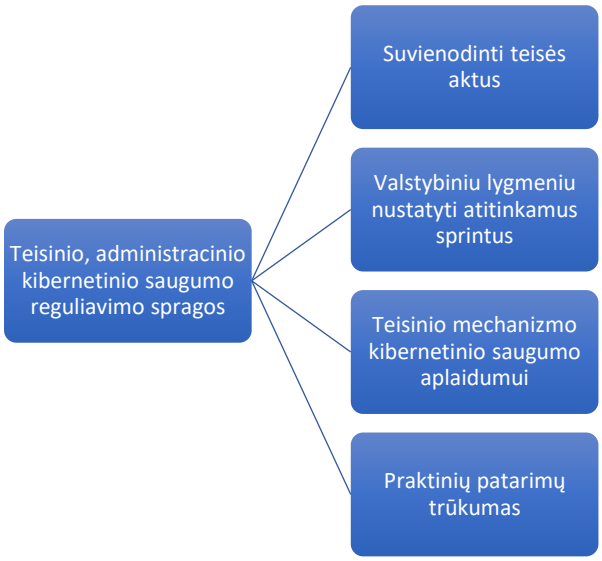
Dar vienas aspektas, kurį išskyrė ekspertai – ***technologijos***. Informantai pabrėžė, jog investavimas į technologijas, personalą, švietimą veikia kaip prevencinės priemonės kibernetiniams nusikaltimams:

technologijos: *„<...> Augant technologijoms auga ir pavojus kibernetiniam saugumui <...>.“* (I 5)
„<...> Didžiausias iššūkis yra padaryti tokią apsaugą, kuri apsaugotų duomenis, slaptažodžius nuo kibernetinių užpuolikų, t.y. apsaugą nuo duomenų nutekėjimo. Dažniausia klaida būna iš vartotojo pusės, kai kenkėjas randa būdu pasisavinti informaciją ne iš sistemos, o iš pačio vartotojo klaidos, kai yra spaudžiamos blogos nuorodos <...>.“ (I 8)

Paskutinis aspektas, kurį išskyrė informantai interviu metu ***bendradarbiavimo trūkumas***. Interviu dalyvavę ekspertai pabrėžė, jog mažai bendradarbiaujama tiek tarp ekspertų, tiek tarp institucijų:

bendradarbiavimo trūkumas: *„<...> Pranešimai viešojoje erdvėje apie naujus atakos tipus ateina pavėluotai, kai nukentėjusių jau būna ne vienas ir ne du. Greitesnis keitimasis informacija ir atakų užkardymas remiantis ja – didžiausias iššūkis <...>.“* (I 7)

Tyrimo metu siekta išsiaiškinti ekspertų nuomonę apie teisinio, administracinio kibernetinio saugumo reguliavimo spragos (15 pav.).



15 pav. Teisinio, administracinio kibernetinio saugumo reguliavimo spragos

Analizuojant tyrimo duomenis buvo išskirtos 4 subkategorijos: ***suvienodinti teisės aktus, valstybiniu lygmeniu nustatyti atitinkamus sprintus, teisinio mechanizmo kibernetinio saugumo aplaidumui, praktinių patarimų trūkumas:***

suvienodinti teisės aktus: *„<...> Teisiniu lygmeniu reikia suvienodinti skirtingų teisės aktų reikalavimus ir prieštaravimus, ypač peržiūrėti Vidaus reikalų ministerijos išleistus teisės aktus <...>.“* (I 1)

Tyrime dalyvavę ekspertai turėjo gana prieštaringą nuomonę apie tai, kokias teisinio, administracinio kibernetinio saugumo spragas jie įžvelgia. Dalies informantų teigimu, jie neįžvelgia teisinio ar/ir administracinio kibernetinio saugumo reguliavimo spragų: *„<...> Kibernetinio saugumo įstatymas bei Nacionalinė kibernetinio saugumo strategija atspindi kibernetinio saugumo reguliavimo sritį <...>.“* (I 2); *„<...> Nieko, tereikia korektiškai vykdyti tai, kas parašyta teisės aktuose ir laikytis standartų <...>.“* (I 4); *„<...> Teisiniame, administraciniame saugumo reguliavimo lygyje, šiuo metu, nieko nepasigedau <...>.“* (I 8). Galima daryti prielaidą, jog nuomonių skirtumą lemia skirtingos patirtys, darbo stažas, darbo vieta, kur yra dirbama. Antras aspektas, kurį išskyrė informantai interviu metu – ***valstybiniu lygmeniu nustatyti atitinkamus sprintus:*** *„<...> Organizaciniame lygmenyje kibernetinį saugumą siūlyčiau efektyvinti ne pilna apimtimi, kaip yra dabar, o valstybiniu lygmeniu nustatyti atitinkamus sprintus (nedidelius iki 2-3 mėn. laiko periodus), kuomet visos organizacijos ir strateginės įmonės privalo susitvarkyti vieną*

kibernetinio saugumo užtikrinimo procesą (pvz. programinės įrangos atnaujinimo procesą) ir vertinti pažangą jame <...>.“ (I 1)

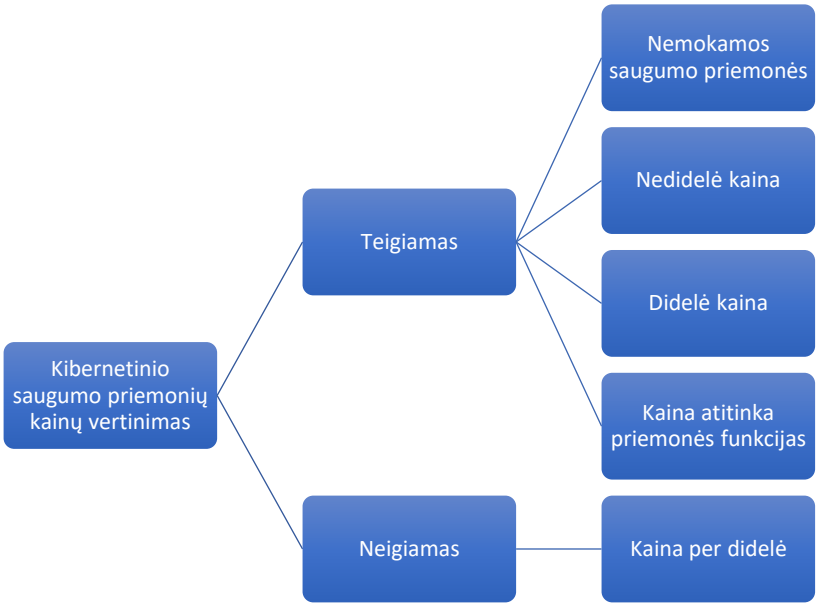
Dar vienas aspektas, kurį išskyrė ekspertai – ***teisinio mechanizmo kibernetinio saugumo aplaidumui***. Informantai pabrėžė, jog investavimas į technologijas, personalą, švietimą veikia kaip prevencinės priemonės kibernetiniams nusikaltimams:

teisinio mechanizmo kibernetinio saugumo aplaidumui: *„<...> Veikiančio teisinio mechanizmo, leidžiančio bausti organizacijų vadovus už nesirūpinimą kibernetiniu saugumu <...>.“* (I 7)

Ketvirtas aspektas, kurį išskyrė informantai interviu metu – ***praktinių patarimų trūkumas***. Interviu dalyvavę ekspertai pabrėžė, jog reiktų kalbėti apie gerąsias, blogąsias praktikas, patarimus:

praktinių patarimų trūkumas: *„<...> praktinių rekomendacijų tipinių sprendimų <...>.“* (I 6)

Analizuojant tyrimo duomenis ekspertai išskyrė 2 subkategorijas – kibernetinio saugumo priemonių kainų vertinimas (16 pav.).



16 pav. Kibernetinio saugumo priemonių kainų vertinimas

Analizuojant tyrimo duomenis buvo išskirtos 2 subkategorijos: ***teigiamas kibernetinio saugumo priemonių kainų vertinimas:***

nemokamos saugumo priemonės: *„<...> yra nemokamų ar santykinai nedaug kainuojančių dalykų, kuriuos naudojant kibernetinis saugumas ženkliai padidėja (pvz.: ryšių (wi-fi, bluetooth) atjungimas jų nenaudojant, dviejų faktorių autentifikacijos naudojimas, saugių slaptažodžių sudarymas, korektiškas jų saugojimas ir naudojimas)* <...>." (I 4);

nedidelės kainos: *„<...> Kibernetinio saugumo užtikrinimo kainos yra didelės tačiau įvertinus kibernetinės atakos pasekmes žala padaryta atakos metu gali būti žymiai didesnė nei kibernetinio saugumo priemonių kaina* <...>." (I 2)

Ekspertai vertindami kibernetinio saugumo priemonių kainą pabrėžė, jog *„<...> Galima, tačiau saugumo priemonių kaina neturėtų būti didesnė už galimos žalos, įvykus kibernetiniam incidentui, kainą* <...>." (I 4). Informantų nuomone, priemonių kainos neturėtų būti didelės. Būtent šie ekspertai skatina atsižvelgti į esamas nemokamas priemones ir/ar priemones, kurių kainos nėra didelės. Vis dėlto šie ekspertai pabrėžia, jog svarbu suprasti, įvertinti, kokie galimi finansiniai nuostoliai įvykus kibernetiniam incidentui. Jei yra tikimybė patirti didelius finansinius nuostolius reiktų, o priemonių tam užkirsti kainos taip pat nėra mažos įmonėms ir įstaigoms vis dėl to reiktų rinktis brangesnes priemones: *„<...> Išlaidos turi būti adekvačios padarytai žalai* <...>." (I 5); *„<...> svarbu užtikrinti stabilų finansavimą. Kibernetinė erdvė yra labai dinamiškai besivystanti sritis, todėl reikalinga nuolat, periodiškai atlikti rizikų vertinimą ir analizuoti/prognozuoti galimas pasekmes. Atitinkamai planuoti reikalingas lėšas, įtikinti vadovus dėl šių investicijų reikalingumo* <...>." (I 6); *„<...> jas renkantis reikia įvertinti kokio rizikos tikimybė, kokia žala būtų jeigu vertinamas įvykis įvyktų, kiek kainuoja priemonės sumažinti riziką. Pagal tai spręsti ar priemonę diegti apsimoka ar ne* <...>." (I 7)

didelė kaina: *„<...> Kibernetinio saugumo užtikrinimo kainos yra didelės tačiau įvertinus kibernetinės atakos pasekmes žala padaryta atakos metu gali būti žymiai didesnė nei kibernetinio saugumo priemonių kaina* <...>." (I 4)

kaina atitinka priemonės funkcijas: *„<...> Kaina dažniausiai būna atitinkama pagal tai, kiek į tai įdėta laiko ir pastangų ir kokias gynybines funkcijas ta sistema atlieka. Kainos yra atitinkamos, nes visos*

sistemos ir jų duomenys yra svarbūs ir brangūs, todėl ir jų saugojimas turi tam atitinkamą kainą. <...>.“ (I 8)

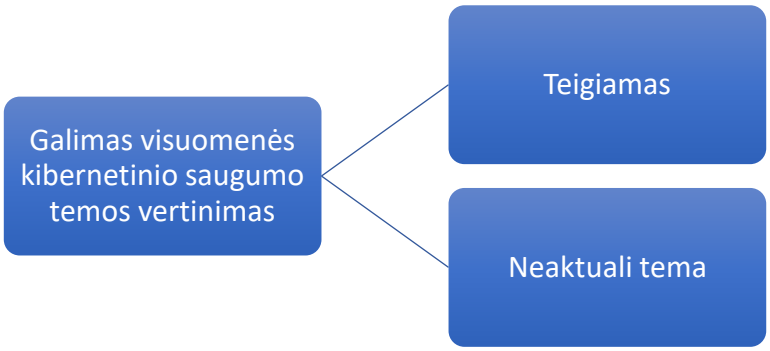
„<...> Kibernetinio saugumo priemonių kaina priklauso nuo priemonių pasirinkimo ir nuo specialistų (kurie dirbs su įrankiais) kvalifikacijos, kompetencijos ir patirties, taip pat nuo infrastruktūros dydžio <...>.“ (I 6)

Ekspertai, kurių teigimu, kibernetinio saugumo priemonių kaina atitinka jų funkcijas taip pat interviu metu pabrėžė, jog *„<...> kibernetinio saugumo priemones reikia rinktis atsižvelgiant į galimas incidentų pasekmes bei to pasekoje patirtą žalą <...>.*“ (I 2). Galima teigti, jog vertinant saugumo priemonių kainas svarbu galvoti apie galimas finansines pasekmes atsitikus incidentui. Vertinant kainą svarbu galvoti, kokius finansinius nuostolius galimai patirs organizacija, įmonė įvykus kibernetiniai atakai.

Antra subkategorija, kurį išskyrė informantai interviu metu - ***neigiamas kibernetinio saugumo priemonių kainų vertinimas:***

kaina per didelė: *„<...> Patikimos saugumo priemonės daug kainuoja nors absoliutaus saugumo nebūna, tiesiog per brangu <...>.*“ (I 5)

Analizuojant tyrimo duomenis išskirtos 2 subkategorijos galimų visuomenės kibernetinio saugumo temos vertinimo (17 pav.).



17 pav. Galimas visuomenės kibernetinio saugumo temos vertinimas

Analizuojant tyrimo duomenis buvo išskirtos 2 subkategorijos: ***teigiamas vertinimas, neaktuali tema:***

teigiamas: *„<...> žiūri labai rimtai ir aiškiai suvokia jos neigiamas pasekmes <...>.“* (I 1)
„<...> Visuomenė turėtų teigiamai vertinti kibernetinio saugumo temą ir skirti tam finansavimą nes tai yra investicija į mūsų visų ateitį. <...>.“ (I 2)

Dar vienas aspektas, kurį išskyrė ekspertai – ***neaktuali tema***. Informantai pabrėžė, jog, jų nuomone, dalis visuomenės nevertina šios temos, jiems ji nėra aktuali. Ši visuomenės dalis nesupranta temos aktualumo ir rimtumo:

neaktuali tema: *„<...> visuomenė per daug rimtai į tai nežiūri. Dauguma net neįsivaizduoja kas yra kibernetinis saugumas, kaip veikia visas pasaulinis interneto tinklas ir kas yra tie kibernetiniai užpuolikai. Tad ir požiūris yra toks, kad kibernetinio saugumo vertinimas yra minimalus <...>.“* (I 8)
*„<...> Dalis visuomenės dar galutinai nesupranta šios tem*os <...>.“ (I 1)

Empirinio tyrimo duomenų analizė atskleidė, jog ekspertai dirbantys kibernetinio saugumo srityje turi skirtingas patirtis ir suvokimus šia tema. Galima daryti prielaidą, jog ekspertų turimas specifines žinias lemia darbo stažas, patirtys tiek dirbant šioje srityje, tiek patirtys susijusios su kibernetinėmis atakomis, incidentais. Ekspertų patirtys atskleidė ir patvirtino, jog kibernetinio saugumo tema darosi vis aktualesnė, todėl būtina pirmiausia skirti dėmesį, atlikti tyrimus, dalintis patirtimi.

IŠVADOS

1. Baigiamojo darbo tema - **Kibernetinio saugumo iššūkiai per kaštų prizmę pasaulyje ir Lietuvoje** išsiskiria vien tik pavadinimu, kaip įdomia ir iššūkių keliančia tyrimų sritimi. Visų pirma tai paaiškinama tuo, kad tema dar nėra pakankamai ištirta, ypač kaštų kontekste. Dėl intensyvių tarptautinių santykių kibernetinėje erdvėje plėtojimo, sąlygojamo, technologijų plėtros greičio ir jų įgyvendinimo valstybių, organizacijų ir asmenų santykiuose, ši sritis visada bus įdomi ir sudėtinga. Tokia išvada daroma dėl nuolatinio požiūrio ir technologijų tobulėjimo. Būtent tas nestabilumas rodo, kad šios temos tyrimų srities per 5 ar 10 metų bus galima padaryti naujas išvadas.
2. Informacinių ir ryšių technologijų plėtra ir prieinamumas bei nuolatinė įtampa tarp skirtingų politiškai ir ideologiškai valstybių sąlygojo tarptautinius santykius virtualioje erdvėje. Strateginio dominavimo virtualioje erdvėje dar nepasiekė nė vienas tarptautinių santykių subjektas. Daugybė tarptautinių subjektų parodė savo buvimą ir norą veikti virtualioje erdvėje. Tai rodo daugiapolį kibernetinės erdvės matmenį, kuriame mažai tikėtina, kad atsiras dominavimas ar šios erdvės pasidalijimas. Tačiau įtakingiausios šalys yra **ekonomiškai** ir kariškai galingiausios, o tuo pačiu ir labiausiai priklausomos nuo kibernetinės infrastruktūros - JAV, Rusija ir Kinija. NATO taip pat vaidina svarbų vaidmenį. Galime daryti išvadą, kad pastaraisiais metais kuriama nauja kibernetinio saugumo samprata, kurią galima apibrėžti kaip kibernetinės erdvės daugiapoliškumo paradigmą.
3. Dauguma autorių prognozuoja konfliktų ir žvalgybinės veiklos virtualioje erdvėje eskalavimą, o tai patvirtina, kad kibernetinės atakos yra viena didžiausių grėsmių tarptautiniam saugumui. Skirtingai nuo įprastų konfliktų, tokie išpuoliai taps vis dažnesni. Todėl būtina sukurti veiksmingą gynybą, kurioje pagrindinis vaidmuo tenka prevencijai, tarptautiniam bendradarbiavimui ir tarptautiniu mastu pripažintų, teisiškai privalomų normų priėmimui.
4. Kokybinis ekpertų tyrimas leidžia daryti išvadas, jog būtinas visuomenės švietimas ir tai turėtų būti prioritetinė sritis. Taip pat eskpertai pasidalino nuomone, jog atsakomybė už aplaidų elgesį su duomenimis taip pat turėtų būti griežtinama. Dažnai susiduriama su nuomone, jog įstaigos, įmonės, institucijos nesiima reikalingų priemonių kibernetiniam saugumui užtikrinti, nes nėra susidūrusios su kibernetinėmis atakomis. Ekspertų nuomone, investicijos į kibernetinį saugumą užtikrina saugumą, kokybę, kompetencijų įgijimo bei tobulinimo galimybes. Investicijos, kibernetinio saugumo srities finansavimas padėtų taip pat užtikrinti visuomenės švietimą šiuo klausimu. **Literatūros šaltinių analizė bei ekspertų interviu atskleidė koreliacijas tarp kibernetinio saugumo ir kaštų.**

REKOMENDACIJOS

1. Kibernetinio saugumo klausimas turi būti laikomas vyriausybės prioritetu, kuriam reikalingi neeiliniai veiksmai. Ypatingas dėmėsys turi būti skiriamas tvirtesnei kibernetinio atsparumo koncepcijai. Kibernetinis atsparumas suteikia keletą aspektų tam, kaip organizacija lieka apsaugota nuolat kintančioje grėsmių aplinkoje. Nors saugumas vis dar yra pagrindinis veiksnys, kibernetinis atsparumas taip pat apima strategijas kibernetinių atakų metu ir iš to kylančių krizių valdymą.
2. Vyriausybė turi taikyti prevencinį požiūrį peržiūrėdama teisės aktus, dokumentus siekiant visapusiškai įvertinti nuolat vykstančius pokyčius šioje srityje. Svarbu atsižvelgti į kibernetinį atsparumą paremtą individualizuotomis sistemomis, leidžiančiomis numatyti grėsmes, atrasti ir įvertinti saugumo incidentų poveikį, siekiant greitai veikti ir priimti pagrįstus sprendimus.
3. Vyriausybė turi sudaryti darbo grupę, kuri padėtų pagerinti analizę duomenų, susijusių su kibernetinio saugumo kaštais, kokybe. Svarbu pagerinti duomenų kokybę šioje srityje, ypatingą dėmesį skiriant visapusiškos išlaidų (finasinių ir kitų) apskaičiavimo sistemos sukūrimui. Atsižvelgiant į šią sistemą, svarbu pateikti rekomendacijas dėl galimų kibernetinio saugumo kaštų planavimo. Tai padėtų įmonėms, organizacijoms bei bendruomenėms geriau įvertinti kibernetinio saugumo kaštus, reikalingus išteklius bei planuotis biudžetus. Darbo grupėje pareigūnai ir teisėsaugos bei kibenretinio saugumo atstovai, turėtų kreipti dėmesį į: numatomas išlaidas, išlaidas kaip pasekmes ir išlaidas reaguojant, kas padėtų suvokti visas kibernetinių saugumo sritis ir galimus kaštus.
4. Vyriausybė turi sukurti mokymo ir švietimo programas visuomenei, kurios padėtų didinti kibernetinį saugumą, ūgdyti visuomenėje kibernetinę „higieną“. Švietimo programas nuolat atnaujinti įvertinant nuolat vykstančius pokyčius šioje srityje.

LITERATŪROS SĄRAŠAS

1. Almarabeh, H., Sulieman, A. (2019). *The impact of cyber threats on social networking sites*. Prieiga per internetą: https://www.researchgate.net/publication/332552039_THE_IMPACT_OF_CYBER_THREATS_ON_SOCIAL_NETWORKING_SITES
2. Baezner, M., Robin, P. (2018). *Cyber and information warfare in the Ukrainian conflict*. Prieiga per internetą: https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict
3. Baezner, M., Robin, P. (2018). *Stuxnet*. Prieiga per internetą:https://www.researchgate.net/publication/323199431_Stuxnet
4. Berg, J. Van Den, Zoggel, J. Van, Snels, M., Leeuwen, M. Van, Boeke, S., Koppen, L. Van De, Bos, T. De. (2014). *On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education*. Prieiga per internetą: https://pdfs.semanticscholar.org/f96e/9e707341baf4eb2784a21cd95b33c41ab685.pdf
5. Bodeau, D., Boyle, S., Fabius-Greene, J., Graubart, R. (2010). *A component of Mitree's cyber prep methodology*. Prieiga per internetą: https://www.mitre.org/sites/default/files/pdf/10_3710.pdf
6. Bojanc, R., Jerman-Blazic, B. (2008). *Towards a standard approach for quantifying an ICT security investment*. Prieiga per internetą: https://doi.org/10.1016/j.csi.2007.10.013
7. Brangetto, P., Kert-Saint Aubyn, M. (2015). *Economic aspects of national cyber security strategies*. Prieiga per internetą: https://ccdcoe.org/uploads/2018/10/Economics-of-cybersecurity.pdf
8. Brookson, C. (2016). *Tackling the challenges of cyber security*. Prieiga per internetą: https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp18_cybersecurity_ed1_final.pdf
9. Cavelty, M. D. (2012). *Cyber-Security*. Prieiga per internetą: https://www.researchgate.net/publication/256018865_Cyber-Security
10. Centre for international governance innovation. (2019). *CIGI-IPOS Global Survey: Internet security and trust*. Prieiga per internetą: https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-

%20Part%201%20%26%202%20Internet%20Security%2C%20Online%20Privacy%20%26%20Trust.pdf

11. *Challenges to effective EU cybersecurity policy*. (2019). Prieiga per internetą: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf
12. *Cyber security research and development agenda*. (2003). Prieiga per internetą: https://web.stanford.edu/class/msande91si/www-spr04/readings/week8/2003_Cyber_Security_RD_Agenda.pdf
13. Cornish, P., Kavanagh, C. (2019). *Geneva dialogue on respinsible behaviour in cyberspace*. Prieiga per internetą: https://genevadialogue.ch/wp-content/uploads/Geneva-Dialogue-Final-Report.pdf
14. Debate security. (2020). Research report. Cybersecurity Technology Efficacy. Prieiga per internetą: https://www.debatesecurity.com/downloads/Cybersecurity-Technology-Efficacy-Research-Report-V1.0.pdf
15. DeSimone, A., Horton, N. (2017). *Sony's nightmare before Christmas. The 2014 North Korean cyber attack on Sony and lessons for US Government actions in cyberspace*. Prieiga per internetą: https://www.jhuapl.edu/Content/documents/SonyNightmareBeforeChristmas.pdf
16. Dynes, S., Goetz, E., Freeman, M. (2008). *Cyber Security: Are Conomic Incentives Adequate?* Prieiga per internetą: https://link.springer.com/chapter/10.1007/978-0-387-75462-8_2
17. Duic,I., Cvrtila, V., Ivanjko, T. (2017). *International cyber security challenges.* Prieiga per internetą: https://bib.irb.hr/datoteka/878827.Duic_Cvrtila_Ivanjko_International_cyber_security_challenges_.pdf
18. *European Commission. Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace*. (2013). Prieiga per internetą: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
19. Fischer, E. A. (2014). *Cybersecurity issues and challenges: in brief*. Prieiga per internetą: https://www.everycrsreport.com/files/20141216_R43831_acbefaafacb64f97fd77df976c469127afdd9308.pdf
20. Gade, N. R., Reddy, U. (2014). *A study of cyber security challenges and its emerging trends on latest technologies*. Prieiga per internetą: https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies

21. Gharibi, W., Mirza, A. (2011). *Security risks and modern cyber security technologies for corporate networks.* Prieiga per internetą: https://arxiv.org/pdf/1105.2002.pdf
22. Hartel, P., Junger, M., Leijtens, A.(2015). *The impact of cyber security on SMEs*. Prieiga per internetą: https://essay.utwente.nl/65851/1/Amrin_MA_EEMCS.pdf
23. Heinl, C., Tan, E. E. (2015). *Cybersecurity: emerging issues, trends, technologies and threats in 2015 and beyond*. Prieiga per internetą: https://www.rsis.edu.sg/wp-content/uploads/2016/04/RSIS_Cybersecurity_EITTT2015.pdf
24. Irandoost, D. H. (2018). *Cybersecurity: a national security issues?* Prieiga per internetą: https://www.e-ir.info/pdf/73942
25. Jang-Jaccard, J., Nepal, S. (2014). *A survey of emerging threats in cybersecurity*. Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S0022000014000178
26. Kahneman, D. (2011). *Thinking, Fast and Slow (Abstract)*. Prieiga per internetą: https://www.researchgate.net/publication/257406325_Kahneman_D_2011_Thinking_Fast_and_Slow#fullTextFileContent
27. Klaic, A. (2015). A *Method for the development of cyber security strategies*. Prieiga per internetą: https://www.researchgate.net/publication/322318207_A_Method_for_the_Development_of_Cyber_Security_Strategies
28. Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., Wolff, S. (1997). *Brief history of the internet*. Prieiga per internetą: https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf
29. Lošonczi, P. (2018). *Importance of Dealing with Cybersecurity Challenges and Cybercrime in the Senior Population*. Prieiga per internetą:https://www.researchgate.net/publication/328848219_Importance_of_Dealing_with_Cybersecurity_Challenges_and_Cybercrime_in_the_Senior_Population
30. McSpaden, S., Appeaning, M. (2017). *Budgeting for cybersecurity*. Prieiga per internetą: https://www.ncsl.org/documents/taskforces/Budgeting_For_Cybersecurity_32041.pdf
31. Nato. (2010). *Strategic concept for the defense and security of the members of the North Atlantic treaty organization*. Prieiga per internetą: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

32. Nato. (2011). *Defending the notworks. The NATO policy on cyber defence*. Prieiga per internetą: https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf
33. Neil, N. F., Neil, M. (2012). *The Need for Causal, Explanatory Models in Risk Assessment.* Prieiga per internetą: http://bayesianrisk.com/sample_chapters/Chapter%202%20The%20need%20for%20causal%20explanatory%20models%20in%20risk%20assessment.pdf
34. Ottis, R. (2018). *Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective.* Prieiga per internetą: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
35. Pande, J. (2017). *Introduction to cyber security*. Prieiga per internetą: http://www.uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf
36. Pardini, D. J., Heinish, A. M. C., Parreiras, F. S. (2017). *Cyber security governance and management for smart grids in Brazilian energy utilities*. Prieiga per internetą: http://www.scielo.br/pdf/jistm/v14n3/1807-1775-jistm-14-03-385.pdf
37. Rowe, B. R., Gallaher, M. P. (2006). *Private Sector Cyber Security Investment Strategies: An Empirical Analysis*. Prieiga per internetą: https://www.researchgate.net/publication/228339552_Private_sector_cyber_security_investment_strategies_An_empirical_analysis
38. Sandar, A. M., Min, Y., Win, K. M. N. (2019). *Fundamental areas of cyber security on latest technology*. Prieiga per internetą: https://www.ijtsrd.com/papers/ijtsrd26550.pdf
39. Schjolberg, S., Ghernaouti-Helie, S. (2009). A global protocol cybersecurity and cybercrime. Prieiga per internetą: https://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf
40. Seemma, P. S., Nandhini, S., Sowmiya, M. (2018). *Overview of cyber security*. Prieiga per internetą: https://www.researchgate.net/publication/329678338_Overview_of_Cyber_Security
41. Soo Hoo, K. J. (2000). *How much is enough? A risk management approach to computer security*. Prieiga per internetą: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/soohoo.pdf
42. Sommestad, T. (2012). *A framework and theory for cyber security assesssments*. Prieiga per internetą: https://www.diva-portal.org/smash/get/diva2:561246/FULLTEXT02.pdf

43. Stosic, L., Veličkovic, D. (2013). *Computer security and security technologies.* Prieiga per internetą: https://www.researchgate.net/publication/282358461_Computer_security_and_security_technologies
44. *The Russo-Georgian war 2008: The role of the cyber attacks in the conflict.* (2012). Prieiga per internetą: https://www.afcea.org/committees/cyber/documents/therusso-georgianwar2008.pdf
45. United Nations. (2004). *Report of the high-level panel on threats, challenges and change. A more secure world: our shared responsability*. Prieiga per internetą: https://daccess-ods.un.org/TMP/9670852.42271423.html
46. United Nations. (1945). *UN Charter*. Prieiga per internetą: https://www.un.org/en/sections/un-charter/un-charter-full-text/
47. Valuch, J. (2017). *Cyber attacks, information attacks, and postmodern warfare*. Prieiga per internetą: https://www.researchgate.net/publication/320761211_Cyber_Attacks_Information_Attacks_and_Postmodern_Warfare
48. Vries, J. (2017). *What drives cyber security investment? Organizational factors and perspectives from decision-makers*. Prieiga per internetą: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=2ahUKEwjZwq6h0u3oAhVJyKYKHWHgC1oQFjAHegQICBAB&url=https%3A%2F%2Frepository.tudelft.nl%2Fislandora%2Fobject%2Fuuid%3A119719ff-cb69-44c5-a566-3ee8373509f7%2Fdatastream%2FOBJ1%2Fdownload&usg=AOvVaw2wxQLNjcXr95sPk3eNoiKW

Mackevičius V. (2021) *Kibernetinio saugumo iššūkiai per kaštų prizmę pasaulyje ir Lietuvoje* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

ANOTACIJA

Magistro baigiamajame darbe išanalizuota kibernetinio saugumo situacija Lietuvoje ir pasaulyje, atskleistos sąsajos tarp kibernetinio saugumo, jo efektyvumo ir kaštų. Pirmame skyriuje atskleidžiama kibernetinio saugumo samprata, kibernetinio saugumo raida bei aktualumas. Antrajame darbo skyriuje yra nagrinėjama transnacionalinio kibernetinio saugumo padėtis pasaulyje, mokslinės literatūros analizės metodu stengiantis atskleisti šių dienų aktualijas ir koreliacijas tarp kibernetinio saugumo užtikrinimo ir kaštų. Trečiajame skyriuje pateikiami tyrimo metodikos pagrindimas, sisteminama kibernetinio saugumo ekspertų pusiau struktūruoto interviu analizė, išskiriant kategorijas ir subkategorijas, analizuojant ir interpretuojant jas. Ketvirtame skyriuje tyrimo metu gautų duomenų pagrindu daromos išvados ir teikiami pasiūlymai, kokių prioritetinių veiksmų imtis LR vyriausybei. Atskleidžiamos tyrimo metu išryškėjusios problemos ir jų sprendimo būdai.

Pagrindiniai žodžiai: kibernetinis saugumas, kaštai

Mackevičius V. (2021) *Challenges of cyber security through the Prism of Costs in the World and in Lithuania* (Master 's Thesis). Vilnius: Mykolas Romeris University

ANNOTATION

The master 's thesis analyzes the cyber security situation in Lithuania and the world, reveals the links between cyber security, its efficiency and costs. The first chapter reveals the concept of cyber security, the development and relevance of cybersecurity. The third chapter presents the rationale for the research methodology, systematizes the analysis of semi-structured interviews of cyber security experts, distinguishing categories and subcategories, analyzing and interpreting them. In the fourth chapter, on the basis of the data obtained during the research, conclusions are made and suggestions are given as to what priority actions to take by the Government of the Republic of Lithuania. The problems revealed during the research and their solutions are revealed.

Key words: cyber security, costs

SANTRAUKA

Valentinas Mackevičius. Kibernetinio saugumo iššūkiai per kaštų prizmę pasaulyje ir Lietuvoje. Magistro baigiamasis darbas / darbo vadovas doc.dr. Marius Laurinaitis; Mykolo Romerio universitetas, Viešojo valdymo ir verslo fakulteto studijų programa. – Vilnius, 2021. – 57 p.

Tyrimo problema – Ar skiriamas pakankamas finasavimas kibernetinio saugumo sektoriui? Ar yra nustatytos koreliacijos tarp kaštų ir kibernetinio saugumo?

Tikslas – Išanalizuoti kibernetinio saugumo kaštų tendencijas Lietuvoje ir pasaulyje.

Uždaviniai: 1. Atskleisti kibernetinio saugumo sampratą; 2. Išanalizuoti transnacionalinio kibernetinio saugumo padėtį; 3. Atlikti kibernetinio saugumo ekspertų interviu siekiant atskleisti kibernetinio saugumo ir kaštų koreliacijas

Metodai: Literatūros šaltinių analizė; pusiau struktūruotas interviu su kibernetinio saugumo ekspertais; turinio (content) analizė.

Tiriamieji: Kibernetinio saugumo ekspertai.

Tyrimo rezultatai: Apibendrinant tyrimų rezultatus galima teigti, jog kibernetinio saugumo ekspertai laikosi vieningos pozicijos, jog ši sritis reikalauja ypatingo dėmesio: žmogiškųjų išteklių, finansinių ir organizacinių resursų bei inovatyvių bei modernių techninių sprendimų. Kibernetinio saugumo ekspertai pasidalino, jog kibernetinio saugumo tikslams pasiekti naudoja įvairias skirtingas priemones jas derindami tarpusavyje. Literatūros šaltinių analizė bei interviu duomenys parodė koreliacijas tarp kaštų ir kibernetinio saugumo efektyvumo.

Magistro baigiamuoju darbu siekiama apžvelgti kibernetinio saugumo situaciją Lietuvoje ir pasaulyje bei ieškoti sąsajų tarp kibernetinio saugumo, jo efektyvumo ir kaštų. Išanalizavus mokslinės literatūros šaltinius, galima teigti, kad finansavimo reikšmė kibernetiniam saugumui - neginčijama. Finansavimas – vienas iš aspektų padedančių užtikrinti rizikų valdymą, prevencijas, ekspertų pritraukimą, visuomenės švietimą šia tema bei suteikia galimybę naudotis inovatyviomis kibernetinio saugumo priemonėmis bei taikyti modernius techninius sprendimus. Straipsnių ir tyrimų analizė atskleidė, kad finansavimas lemia ne tik saugumą, tačiau ir kokybės užtikrinimą, kompetencijų įgijimo bei tobulinimo galimybes. Tiek autoriai, tiek tyrimas parodė koreliacijas tarp finansavimo kibernetiniam saugumui užtikrinti bei jo efektyvumo.

SUMMARY

Valentinas Mackevičius. Challenges of cyber security through the prism of costs in the world and in Lithuania. Master's Thesis / Supervisor doc.dr. Marius Laurinaitis; Mykolas Romeris University, Faculty of Public Administration and Business study program. - Vilnius, 2021. - 57 p.

Research issue. Is funding for the cyber security sector sufficient enough? Are there any correlations between cost and cyber security?

The aim is to analyze the trends in cyber security costs in Lithuania and the world.

Tasks. 1. To reveal the concept of cyber security; 2. To analyze the situation of transnational cyber security; 3. Conduct interviews with cyber security experts to reveal the correlations between cyber security and costs.

Methods. Analysis of literature sources; semi-structured interviews with cyber security experts; content analysis.

Subjects of research. Cyber security experts.

Research results. Summarizing the research results, it can be stated that cyber security experts agree that this area requires special attention to human resources, as well as financial, organizational resources, innovative and modern technical solutions. Cyber security experts stated that they use a variety of different tools to achieve cyber security goals by combining them with each other. Analysis of literature sources and interview data showed correlations between cost and cyber security effectiveness.

The aim of the master's thesis is to review the cyber security situation in Lithuania and the world and to look for connections between cyber security, its efficiency and costs. After analyzing the sources of scientific literature, it can be stated that the significance of funding cyber security is indisputable. Funding is one of the aspects that helps to ensure risk management, prevention, attracts experts, educates society and provides access to innovative cyber security tools and modern technical solutions. The analysis of articles and research revealed that funding determines not only security, but it also assures quality, opportunities for improvement and the acquisition of competencies. Both the authors and the study have shown correlations between funding cyber security and its effectiveness.

1 PRIEDAS

Tyrime panaudotas interviu protokolas

KIBERNETINIO SAUGUMO IŠŠŪKIAI PER KAŠTŲ PRIZMĘ
PASAULYJE IR LIETUVOJE
EKSPERTŲ APKLAUSA

Interviu protokolas

Sveiki, esu Valentinas Mackevičius, Mykolo Romerio universiteto Viešojo valdymo ir verslo fakulteto Kibernetinio saugumo valdymo programos studentas. Šiuo metu rengiu baigiamąjį magistro darbą ir atlieku tyrimą, kurio tikslas –**„Nustatyti kaip kibernetinio saugumo ekspertai vertina situaciją kibernetiniam saugumui per kaštų prizmę pasaulyje ir Lietuvoje“**

A. BENDRI DUOMENYS:

1. Darbovietės pavadinimas (jei gali, teikia).....
2. Užimamos pareigos (jei gali, teikia)…….
3. Darbo stažas (metais)……

B. EKSPERTŲ KIBERNETINIO SAUGUMO LIETUVOJE VERTINIMAS:

1. Kaip vertinate kibernetinio saugumo temą? Kodėl?

_____

_____

_____

_____

_____

2. Kaip įvertintumėte pasiruošimą atremti kibernetines atakas? (Jeigu galite pateikite keletą pavyzdžių)

_____

_____

3. Kokias žalas dažniausiai patiriame dėl saugumo pažeidimų atvejų?

_____

_____

_____

_____

_____

4. Ko pasigendate iš techninių kibernetinio saugumo priemonių šalyje? Kodėl? (Jeigu galite pateikite pavyzdžių)

_____

_____

_____

_____

_____

5. Kaip vertinate kibernetinio saugumo priemonių kainą? Kodėl? (Jeigu galite pateikite pavyzdžių).

_____

_____

_____

_____

_____

6. Ar galima sieti kibernetinio saugumo išlaidas su incidentų pasekmėmis bei žala? Kodėl?

_____

_____

_____

_____

_____

7. Kaip vertinate investicijas į kibernetinį saugumą? Kodėl?

_____

8. Ko pasigendate teisiniame, administraciniame kibernetinio saugumo reguliavimo lygyje?

9. Su kokiais iššūkiais susiduria pasaulis kalbant apie kibernetinį saugumą? (Jeigu galite pateikite pavyzdžius).

10. Kokie veiksniai padeda užtikrinti kibernetinį saugumą? (Jeigu galite pateikite pavyzdžius).

11. Kaip Jūsų nuomone visuomenė vertina kibernetinio saugumo temą ir kibernetinio saugumo finansavimą?

Nuoširdžiai dėkoju už Jūsų atsakymus!

Interviu atliko Valentinas Mackevičius, Mykolo Romerio universiteto studentas.

valemackys@gmail.com