MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

VILTĖ PETKEVIČIŪTĖ

E. VALDŽIOS SISTEMŲ TOBULINIMAS NACIONALINIO KIBERNETINIO SAUGUMO KONTEKSTE: PASAULINĖ PATIRTIS IR LIETUVOS PERSPEKTYVA

Magistro baigiamasis darbas

Vadovas

Prof. dr. T. Limba

VILNIUS, 2022

MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

E. VALDŽIOS SISTEMŲ TOBULINIMAS NACIONALINIO KIBERNETINIO SAUGUMO KONTEKSTE: PASAULINĖ PATIRTIS IR LIETUVOS PERSPEKTYVA

Kibernetinio saugumo valdymo magistro baigiamasis darbas

Studijų programa 6211LX066

Vadovas

Prof. dr. T. Limba

2022 12 …

Atliko

V. Petkevičiūtė KSVvmis20-1 stud.

2022 12 …

VILNIUS, 2022

TURINYS

LENTELĖS

PAVEIKSLAI

SANTRUMPŲ SĄRAŠAS

BNS- Baltics News Service;

DDoS (angl. *Distributed Denial of Service)* ataka– paskirstyta paslaugos trikdymo ataka;

DoS (angl. *Denial of Service*) ataka- atkirtimo nuo paslaugos ataka;

EGDI (*angl.* E-Government Development Index)- Elektroninės valdžios raidos indeksas;

IoT (angl. *Internet of Things*)- daiktų internetas;

IRT- Informacinės ir ryšių technologijos;

IS- Informacinės sistemos;

IT- Informacinės technologijos;

LR- Lietuvos Respublika;

NKSC- Nacionalinis kibernetinio saugumo centras;

RDoS (angl. *Ransom Denial of Service)* - išpirkos reikalaujanti ataka;

RRT- Ryšių reguliavimo tarnyba;

VMI- Valstybinė mokesčių inspekcija.

SĄVOKŲ SĄRAŠAS

Elektroninė valdžia - visuma viešojo administravimo veikloje diegiamų informacinių ir ryšių technologijų (IRT), organizacinių šios veiklos pokyčių ir naujų įgūdžių, skirtų viešosioms paslaugoms, demokratiniams procesams ir viešajai politikai tobulinti.

Elektroninė viešoji paslauga – tai teisės aktais reglamentuojama viešojo administravimo subjektų veikla, skirta teisės subjektams už užmokestį arba nemokamai, padėti įgyvendinti jų teises bei vykdyti pareigas, nuotoliniu būdu, naudojant informacines ir telekomunikacines technologijas, jiems teikiant ir iš jų priimant duomenis, informaciją bei dokumentus.

Elektroniniai valdžios vartai – internetinis portalas, kurio pagrindinė paskirtis yra vieno langelio principu teikti visų valstybės institucijų viešąsias elektronines paslaugas.

Interoperabilumas – kelių sistemų, kompiuterių arba programų gebėjimas keistis duomenimis ir pasinaudoti tais duomenimis.

Ypatingieji duomenys - (angl. *Sensitive Data*)- duomenys, kurių atskleidimas arba netinkamas panaudojimas gali turėti žalingų pasekmių.

ĮVADAS

Temos aktualumas ir naujumas. Šiandieninėje visuomenėje naudojimasis informacinėmis technologijomis (IT) smarkiai išaugo. Ko gero daugelis iš mūsų net nepastebėjome, kaip visas gyvenimo sritis (ekonomiką, švietimą, politiką, teisę, viešąjį administravimą ir kt.) apjungė internetas. Modernėjant visuomenei, modernėja ir viešasis valdymas- vis daugiau viešųjų ir administracinių paslaugų yra prieinama internete. Remiantis Informacinės visuomenės plėtros komiteto statistika (2021), nuo 2017 iki 2020 metų atsirado dar 19 viešųjų ir administracinių paslaugų, teikiamų internetu. Pasak Augustinaičio, Rudzkienės, Petrausko ir kt. (2009), šiuolaikinis viešasis valdymas tampa vienu iš svarbiausių globaliojo konkurencingumo veiksniu. Dar labiau padidėjusį informacinių sistemų naudojimą lėmė ir pasaulinė COVID-19 pandemija, kuomet norint išvengti žmogiško kontakto ir užsikrėtimo virusu, daugelis gyvenimo sričių persikėlė į kibernetinius tinklus. Tačiau augant viešųjų ir administracinių paslaugų, kurias galima atlikti internetu kiekiui, didėja ir kibernetinių atakų skaičius. Pagal 2020 metų ataskaitą, kibernetinių nusikaltimų skaičius išaugo 25%. Prie kibernetinių nusikaltimų suaktyvėjimo prisidėjo ir COVID- 19 pandemija, nes daugeliui darbuotojų pradėjus dirbti iš namų, nusikaltėliams pažeisti jų privatumą kibernetinėje erdvėje tapo dar lengviau. 2020 metų balandį fiksuotas išaugęs grasinimų sutrikdyti paslaugas skaičius, prašant išpirkos- RDDoS, (angl. *Ransom Denial of Service*). Taip pat papildomai buvo vykdomos demonstracinės kibernetinės atakos (KAM, 2020). Todėl tikslas apsaugoti piliečius ir valstybę nuo kibernetinių atakų dar labiau išaugo. Kibernetinių incidentų valdymas tampa ne vien Lietuvos, bet ir visos Europos problema. Kibernetinio saugumo išpuoliai kelią didelę grėsmę tarptautiniam saugumui, taip pat valstybės ekonominei, socialinei ir politinei plėtrai. Kenkėjiški veiksmai, nukreipti prieš ypatingos svarbos infrastruktūros objektus, kelia didžiulę pasaulinę riziką (Europos komisija, 2020).

Mokslinė problema. Norint įgyvendinti kibernetinio saugumo politiką Lietuvoje dažnai susiduriama su piliečių bei viešojo sektoriaus darbuotojų abejingumu kibernetinio saugumo praktikai. Dėl žinių trūkumo ar negebėjimo pritaikyti turimų žinių, susijusių su kibernetiniu saugumu, praktikoje įvyksta taip vadinama žmogiškoji klaida, kuri yra silpnoji vieta kibernetinio saugumo užtikrinime. Mokslo šaltiniuose dažniausiai analizuojami ir didžiausi akcentai dedami verslo sektoriaus kibernetiniam saugumui užtikrinti, o viešojo sektoriaus saugumas tampa ne prioritetine pozicija. Pagrindinė problema- viešojo sektoriaus ir elektroninės valdžios sistemų kibernetinio saugumo spragos yra per mažai išanalizuotos ir ištyrinėtos.

Tyrimo objektas. Elektroninės valdžios ir jų sistemų saugumo įgyvendinimas Lietuvoje bei pasaulyje.

Tikslas- Remiantis literatūra bei teisiniais dokumentais, išanalizuoti elektroninės valdžios tobulinimo galimybes Lietuvoje ir atskleisti kaip užtikrinamas šalies elektroninių valdžios vartų kibernetinis saugumas bei pateikti su šia sritimi susijusias rekomendacijas ir pasiūlymus.

Uždaviniai:

1. Išanalizuoti elektroninės valdžios sistemų kūrimą ir diegimą teoriniu aspektu;
2. Atlikti E. valdžios kūrimo ir diegimo pasaulinės patirties analizę;
3. Išnagrinėti kibernetinio saugumo užtikrinimo elektroninės valdžios informacinėse sistemose aspektus;
4. Atlikti elektroninės valdžios sistemų tobulinimo nacionalinio kibernetinio saugumo kontekste kokybinį tyrimą LR Klaipėdos apygardos prokuratūroje bei Lietuvos didžiojo kunigaikščio Butigeidžio dragūnų batalione ir sužinoti ekspertų nuomonę apie kibernetinio saugumo klausimą šiose valstybinėse institucijose.

Duomenų rinkimo metodai ir analizė.

Rašant magistro darbą buvo atliekama mokslinės literatūros ir dokumentų turinio, teisės aktų analizė bei atlikta dviejų susijusių grupių ekspertų apklausa. Darbe buvo atliktos teorinė aprašomoji, sisteminė ir lyginamoji analizės. Ekspertų nuomonę siekiama sužinoti standartizuoto interviu arba kitaip klausimyno forma. Magistriniame darbe siekiant išsiaiškinti teorinius elektroninės valdžios kūrimo, vystymosi, įgyvendinimo ir tobulinimo aspektus buvo taikyta mokslinės literatūros analizė. Statistinių duomenų analizės metodas buvo taikomas siekiant išskirti dvi šalis atvejo analizei. Buvo pasirinktos dvi šalys: viena Europos Sąjungos šalis (Danija) ir viena Okeanijos regiono šalis (Naujoji Zelandija), kurių gerąją kibernetinio saugumo kūrimo ir tobulinimo praktiką būtų galima pritaikyti Lietuvoje. Pasirinkus atvejo analizės metodą siekta išskirti atrinktų šalių elektroninės valdžios praktikos pritaikomumą Lietuvoje. Taip pat siekiant išsiaiškinti įvairių grupių (prokurorų bei karininkų) nuomonę, atliktas kokybinis tyrimas. Tyrimu siekta išsiaiškinti su kokiomis kibernetinio saugumo problemomis susiduria valstybinio sektoriaus darbuotojai.

Darbo struktūra.

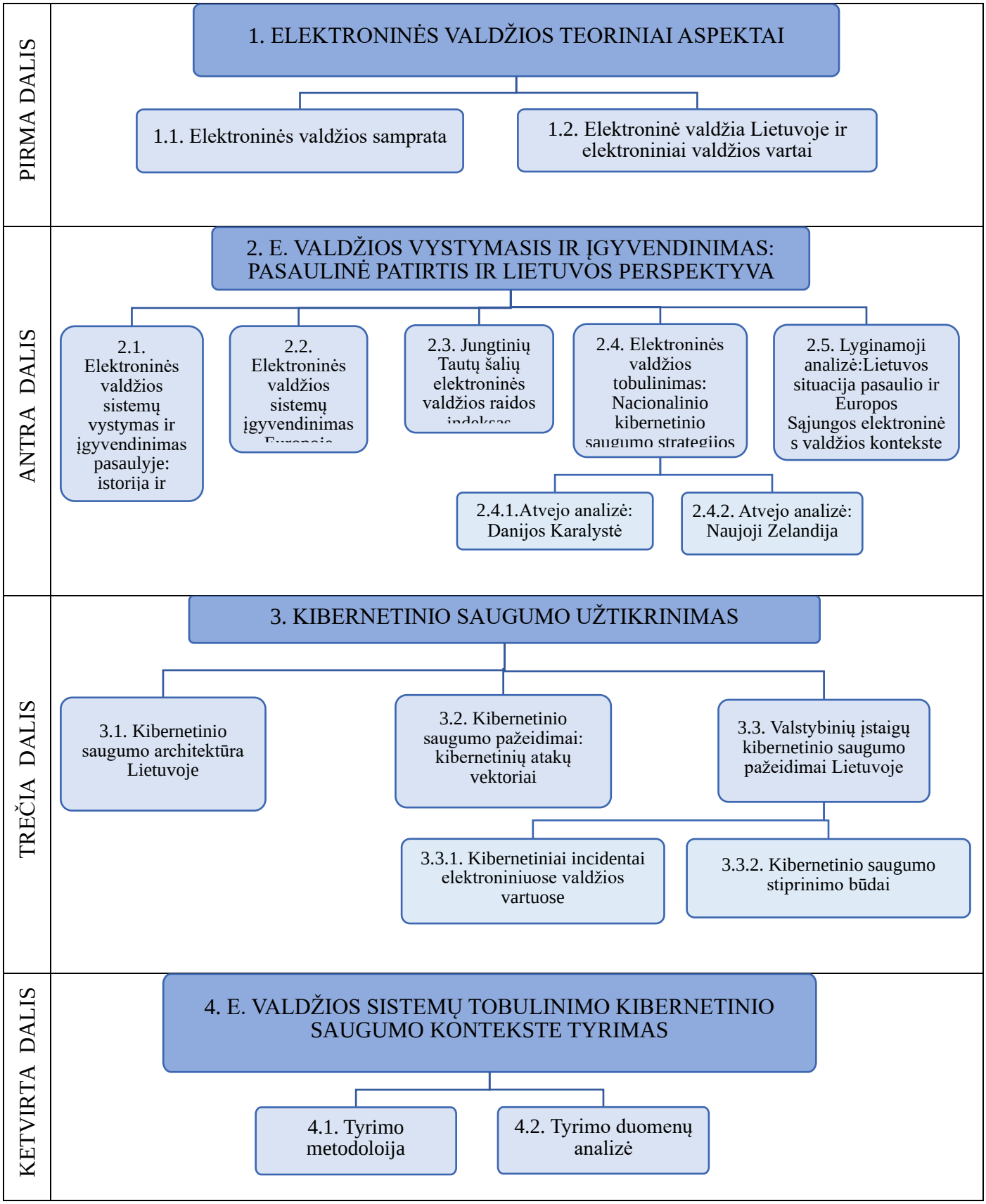
Magistro darbą sudaro 4 dalys (žr. 1 pav.). Pirmoje darbo dalyje nagrinėjami elektroninės valdžios teoriniai aspektai: elektroninės valdžios samprata, e. valdžia Lietuvoje ir elektroniniai valdžios vartai. Antroje dalyje analizuojamas elektroninės valdžios sistemų vystymas ir įgyvendinimas pasaulyje bei Europoje, Jungtinių Tautų elektroninės valdžios raidos indeksas, elektroninės valdžios tobulinimas. Pateikiama lyginamoji analizė- Danijos Karalystės ir Naujosios Zelandijos pavyzdžiai bei Lietuvos situacija pasaulio ir ES kibernetinio saugumo kontekste. Trečioje dalyje nagrinėjama Lietuvos kibernetinio saugumo architektūra, saugumo pažeidimai, labiausiai pažeidžiami sektoriai bei kibernetinio saugumo pažeidimai valstybinėse įstaigose. Ketvirtoje dalyje nagrinėjamas atliktas tyrimas, kurio tikslas - pasitelkiant ekspertų žinias, išsiaiškinti kaip dažnai valstybinėse įstaigose atliekamos kibernetinio saugumo pratybos, ar darbuotojai tiesiogiai susiduria su grėsmėmis ir ar jiems žinoma ką daryti pastebėjus kibernetinį nusikaltimą jų darbovietėje.

D**arbo praktinis reikšmingumas.**

Saugumo internete, o ypač kibernetinio saugumo e. valdžioje tema labai aktuali, tačiau dar ne tiek daug tyrinėta. Romanosky (2016) aiškinosi 2013 metais JAV prezidento pasirašytą nutarimą, kuriame svarbiausiu aspektu laikomas šalies kibernetinis saugumas ir tam užtikrinti reikia kurti apsaugos sistemas. Limba, Gulevičiūtė (2013) analizavo e. valdžios paslaugų diegimo ypatumus Europos Sąjungoje ir Lietuvoje. Štitilis (2013) atliko tyrimą, kuris atskleidė, jog Lietuvos kibernetinio saugumo strategija per daug abstrakti ir joje ne užtikrinami pagrindiniai ES strategijoje keliami uždaviniai. Plečkaitis (2016) tyrė kibernetinių atakų poveikį Lietuvai. Petronytė (2019) nustatė, kad Lietuvoje kibernetinio saugumo įgyvendinimas yra nukreiptas į tris pagrindines kryptis- saugumo stiprinimo, nusikalstamumo mažinimo ir bendradarbiavimo skatinimo. Pasak tyrėjos Petronytės (2019), įgyvendinant kibernetinio saugumo politiką Lietuvoje yra susiduriama su didelėmis bendradarbiavimo problemomis.

Šiame magistriniame darbe siekiama išgryninti kokiais aspektais galima tobulinti elektroninės valdžios Lietuvoje kibersaugumą. Remiantis Danijos bei Naujosios Zelandijos gerąja praktika bei Lietuvos ekspertų įžvalgomis bus parengti pasiūlymai ką ir kaip galima būtų patobulinti, kad elektroninė valdžia išvengtų kibernetinių atakų.

Magistro baigiamojo darbo loginė schema.



1 pav. Baigiamojo magistro darbo loginė schema

1. ELEKTRONINĖS VALDŽIOS KŪRIMO IR DIEGIMO TEORINIAI ASPEKTAI

1.1. Elektroninės valdžios samprata

Nors demokratija pasaulyje įsivyravo dar Senovės Atėnų laikais, elektroninė valdžia (toliau e. valdžia) neturi tokių senų ištakų. Naudojimasis informacinių ir ryšių technologijomis prasidėjo dar 1950-1960 metais. Tas laikotarpis laikomas mokslinio administravimo pradžia. Tačiau elektroninės valdžios sąvoka, tokia, kokią mes suprantame šiandien atsirado tik 1990 metų pradžioje, kuomet įvyko bendra liberalų demokratinių politinių sistemų viešojo sektoriaus reforma (Chadwich, 2016). Dešimtojo dešimtmečio vidurys laikomas interneto naudojimo "sprogimu", o 1997 metais Jungtinėje Karalystėje išrinkta leiboristų partija savo modernėjančios vyriausybės programoje akcentavo elektroninių paslaugų teikimą (Chadwich, 2016). Nors nuo sąvokos atsiradimo praėjo keli dešimtmečiai, mokslinėje literatūroje dar iki šiol nėra iki galo bendro sutarimo kokiu kampu reikėtų nagrinėti elektroninę valdžią, nes ji yra nuolatinės kaitos būsenoje (Chadwich, 2016). Todėl analizuojant literatūrą galima pastebėti skirtingus požiūrius ir pjūvius, kurie dažniausiai išskiria vieną ar daugiau e. valdžios nagrinėjimo aspektų. Per ilgą viešojo administravimo mokslo laikotarpį nusistovėjo keletas esminių elektroninės valdžios sąvokų, tačiau viena bendrai suvokiama sąvoka vis dar yra diskutuojama. Tam, kad toliau galėtume nagrinėti elektroninės valdžios įgyvendinimą ir saugumą, reikia aptarti pagrindinius e. valdžios apibrėžimus, kuriuos skirtingi šaltiniai pateikia skirtingai:

Elektroninė valdžia- tai informacinių technologijų (IT) taikymas vyriausybės veiklai ir viešosioms paslaugoms bei naujų komunikacijos ryšių tarp valdžios ir piliečių kūrimas (Caves, 2005, p. 180).

Elektroninė valdžia gali būti suvokiama ir kaip informacinių technologijų pritaikymas modernizuojant valstybės valdymą, politiką ir strategijas. Taip pat e. valdžia gali būti įvardijama ir kaip vienas iš būdų pagerinti visuomenės ir valdžios komunikavimo kokybę, modernizuoti valstybės valdymą, sėkmingai vykdyti valstybės reformą, prisitaikant prie visuomenės reikalavimų (Kiškis ir Limba, 2004, p. 34) .

Vienas iš teorinio analizavimo būdų, šiuo atveju elektroninės valdžios analizei, tai visumos skirstymas į modelius. Dažniausiai literatūroje išskiriami trys pagrindiniai elektroninių paslaugų diegimo modeliai pagal vartotojų grupes:

- Valdžia - gyventojams (G2C);
- Valdžia - valdžiai (angl. G2G);
- Valdžia - verslui (angl. G2B) (Yadav ir Singh, 2012).

Pasak Yadav ir Singh, (2012), valdžia - gyventojams valdymo modelis apima viešąsias paslaugas, kurios reikalingos piliečiams. Tai tokios paslaugos kaip:

- Sąskaitų už elektrą, vandenį apmokėjimas internetu; telefono sąskaitos ir kt.
- Paraiškų registracija internetu;
- Įrašų kopijos, deklaravimai internetu;
- Skundų pildymas internetu;
- Bet kokios rūšies internetinės informacijos prieinamumas.

Valdžia - valdžiai (G2G) modelis nurodo paslaugas, kuriomis dalijasi viešojo valdymo įstaigos. Tai yra informacija, kurios sklaida reikalinga norint užtikrinti sklandų ir skaidrų tarpinstitucinį darbą. Šie paslaugų ar informacijos tipai yra tokie:

- Dalijimasis informacija tarp policijos departamentų ir kitų valstybės institucijų;
- Vyriausybės dokumentų keitimas, kuris apima dokumentų paruošimą, patvirtinimą, platinimą ir saugojimą;
- Visi vyriausybiniai dokumentai taip pat pateikiami ir apdorojami per elektroninio valdymo sistemas;
- Didžioji dalis finansinių ir biudžetinių klausimų taip pat tvarkomi per e. valdžios sistemas (Yadav ir Singh, 2012).

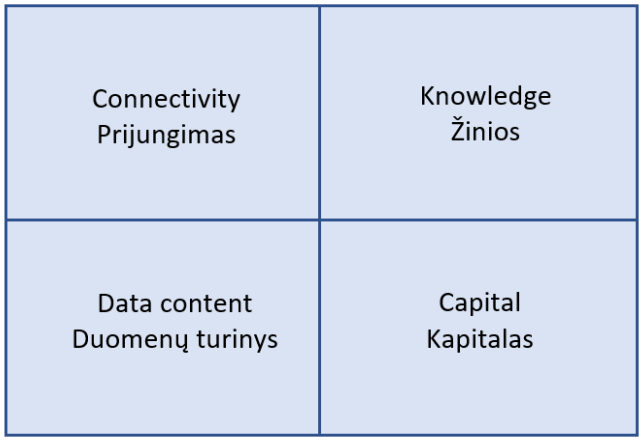
Valdžia - verslui (G2B): naudojant šį modelį ryšys tarp privataus sektoriaus ir vyriausybės didėja ir verslininkai naudojasi bendravimui. Jie dalijasi informacija per šį modelį kaip:

- Mokesčių surinkimas.
- Taip pat atliekamas patento patvirtinimas arba atmetimas;
- Įvairių rūšių sąskaitų ir baudų apmokėjimas;
- Dalijimasis informacija ir duomenimis;
- Skundai ir panašiai (Yadav ir Singh, 2012).

Garuckas ir Kaziliūnas (2008) teigė, kad valdžia - valdžiai modelis daugeliu atžvilgių yra elektroninės valdžios pagrindas, ir valdžia, norėdama sėkmingos elektroninės komunikacijos su piliečiais, pirmiausia turi tobulinti ir modernizuoti savo vidaus sistemą bei procedūras (Garuckas ir Kaziliūnas, 2008). Autorių teigimu, e. valdžią apibendrinantis ir esminis požiūris yra bendradarbiaujantis valdymas (angl. *collaborative governance*). Todėl šiuolaikinės elektroninės

valdžios tęstinio kūrimo pagrindas turėtų būti adaptyvi bendradarbiaujančio valdymo sistema, kurioje dera vidinė integracija ir reagavimas į aplinkos pokyčius (Garuckas ir Kaziliūnas, 2008).

E. valdymas: vyriausybė naudojasi elektroninėmis sistemomis teikiant savo paslaugas internetu nuo pradžios iki galo. E. valdymo tikslas, kad sistemomis naudotųsi kuo didesnė visuomenės dalis, taip pat ir verslas bei valstybinės organizacijos ir įstaigos. Yadav ir Singh (2012) išskyrė keturis elektroninio valdymo ramsčius:



2 pav. Elektroninio valdymo ramsčiai
Šaltinis: Yadav ir Singh (2012)

1. PRIJUNGIMAS: Ryšys reikalingas norint efektyviai atlikti elektroninį valdymą, kad e. valdymas būtų veiksmingas, turi būti stiprus ryšys.

2. ŽINIOS: Žinios čia reiškia IT žinias: Vyriausybė turėtų įdarbinti kvalifikuotus inžinierius, kurie galėtų veiksmingai tvarkyti e. valdymą, taip pat rasti būdus kaip visapusiškai išnaudoti turimus įgūdžius, nuolat ieškoti efektyvesnių alternatyvų elektroninio viešojo valdymo įgyvendinimui.

3. DUOMENŲ TURINYS: Tam, kad būtų paprasta dalintis žiniomis ir informacija internete, turi būti kuriamos duomenų bazės. Duomenų bazėse turėtų būti duomenys susiję su viešojo valdymo paslaugomis.

4. KAPITALAS: Kapitalas gali būti viešasis arba privatus. Tai reiškia pinigus, kuriuos vyriausybė naudoja savo paslaugoms teikti arba ekonomikai kelti (Yadav ir Singh, 2012).

Nors į elektroninės valdžios sąvoką galima pažiūrėti skirtingais kampais, pagrindinė elektroninės valdžios ypatybė yra tai jog naudojant informacines technologijas siekiama glaudaus ir inovatyvaus valdžios, verslo ir visuomenės bendradarbiavimo elektroninė erdvėje. Taigi, sukonkretinus kas yra

elektroninė valdžia ir kokie pagrindiniai jos ramsčiai galime daryti išvadą, kad šiuolaikiniam viešajam valdymui tai svarbus aspektas norint tobulinti valstybės valdymą ir vykdyti reformas siekiant būti inovatyvia ir kibernetiškai stipria valstybe ne tik Europos, bet ir pasaulio kontekste.

1.2. E. valdžios vartų sistemų analizė

Elektroniniai valdžios vartai tai administracinių ir viešųjų elektroninių paslaugų portalas, kuris skirtas gyventojams, verslo įmonėms ir paslaugų teikėjams. Siekiant sudaryti kuo geresnes sąlygas valstybės informacinėms sistemoms ir valstybiniams registrams keistis duomenimis naudojantis žiniatinklio paslaugomis (angl. *Web Services*). Elektroniniai valdžios vartai taip pat padeda ne tik centralizuotai teikti viešąsias elektronines paslaugas, bet ir skatina sparčiau kurti ir integruoti naujas paslaugas (Informacinės visuomenės plėtros komitetas, 2018).

Todėl 2008 m. buvo sukurta ir įdiegta Viešojo administravimo institucijų informacinių sistemų interoperabilumo (sąveikumo) sistema (VAIISIS). Sistema buvo sudaryta iš dviejų dalių:

centrinio elektroninių paslaugų portalo „Elektroniniai valdžios vartai“ (www.epaslaugos.lt, www.evaldzia.lt, www.govonline.lt) ir duomenų mainų platformos.

Nuo 2013 m. kovo 1 d. VAIISIS pavadinimas pakeistas į Valstybės informacinių išteklių sąveikumo platforma (VIISP) (Informacinės visuomenės plėtros komitetas, 2018). Elektroninius valdžios vartus sukūrė ir administruoja Informacinės visuomenės plėtros komitetas, veikiantis prie Susisiekimo ministerijos.

Portalo adresas internete – https://www.epaslaugos.lt/portal/.

Pradiniame puslapyje matomos trys skiltys pagrindinėms naudotojų grupėms prisijungti:

- Fiziniams asmenims;
- Juridiniams asmenims;
- Viešajam sektoriui.

Norint prisijungti prie portalo ir naudotis elektroninėmis paslaugomis reikia patvirtinti savo tapatybę. Tai galima padaryti dviem būdais:

- Pasinaudojant bankų elektroninės bankininkystės sistemomis:

Elektroninė bankininkystė plačiąja prasme suprantama kaip sistema, kuri suteikia galimybę fiziniams ar juridiniams asmenims atlikti įvairius mokėjimo pavedimus, valdyti sąskaitas. Elektroninės bankininkystės sistemos taip pat leidžia patvirtinti savo tapatybę internete Smart - ID, biometrika, PIN generatoriumi arba mobiliuoju parašu.

- Pasinaudojant elektroniniu parašu:

Europos Sąjungos elektroninės atpažinties reglamente pateikiama tokia sąvoką: ”Elektroninis parašas– elektroninės formos duomenys, kurie yra prijungti prie kitų elektroninės formos duomenų arba logiškai susieti su jais ir kuriuos pasirašantis asmuo naudoja pasirašydamas” (Europos Parlamentas ir ES Taryba, 2014). Elektroninio parašo, kaip elektroninių operacijų patikimumo užtikrinimo paslaugą, kūrimą, tikrinimą, galiojimą, parašo naudotojų teises ir atsakomybę reglamentuoja eIDAS reglamentas ir Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymas (Lietuvos Respublikos vidaus reikalų ministerija, 2020). eIDAS tai reglamentuota elektroninė identifikavimo ir autentifikavimo paslauga, skirta užtikrinti, kad elektroninė erdvė būtų saugesnė, greitesnė ir veiksmingesnė visoje Europos Sąjungoje. eIDAS siekiama, kad elektroninės paslaugos būtų vykdomos sklandžiai ir saugiai nepaisant to, kurioje ES valstybėje atliekamos. Todėl sukurta bendra elektroninio identifikavimo sistema- eID ir patikimumo užtikrinimo paslaugų sistema tam, kad paslaugų teikimas visoje Europos Sąjungoje būtų paprastesnis ir vientisas (European Commission, 2022).

eIDAS skatina visų ES šalių interoperabilumą (sąveikumą) elektroninėje erdvėje siekiant, kad šalys pripažintų ir patvirtintų viena kitos elektroninio identifikavimo schemas. Interoperabilumas suprantamas kaip įvairių organizacijų ir sistemų sugebėjimas veikti (dirbti) kartu. Interoperabilumas svarbus todėl, kad leidžia sklandžiai kartu veikti skirtingiems komponentams ir yra kertinis instrumentas e. valdžios tikslams pasiekti. Galimybė skaidyti komponentais ir tuos komponentus jungti svarbi konstruojant dideles ir sudėtingas sistemas, o be interoperabilumo tai tampa beveik neįmanoma.

eIDAS taikomas:

- Elektroninės atpažinties schemoms, apie kurias Europos Komisijai pranešė ES šalys;
- ES įsisteigusiems patikimumo užtikrinimo paslaugų teikėjams (Europos Sąjungos leidinių biuras, 2016).

Taigi, prie elektroninių valdžios vartų patogu prisijungti per įvairius išmaniuosius įrenginius iš bet kurios pasaulio vietos kur yra interneto prieiga. Dėka elektroninio prisijungimo, vartotojas gali nenutrūkstamai naudotis e. valdžios portalų paslaugomis.

2. PASAULINĖ PATIRTIS IR LIETUVOS PERSPEKTYVA

2. 1. Elektroninės valdžios sistemų vystymas ir įgyvendinimas pasaulyje: istorija ir patirtis

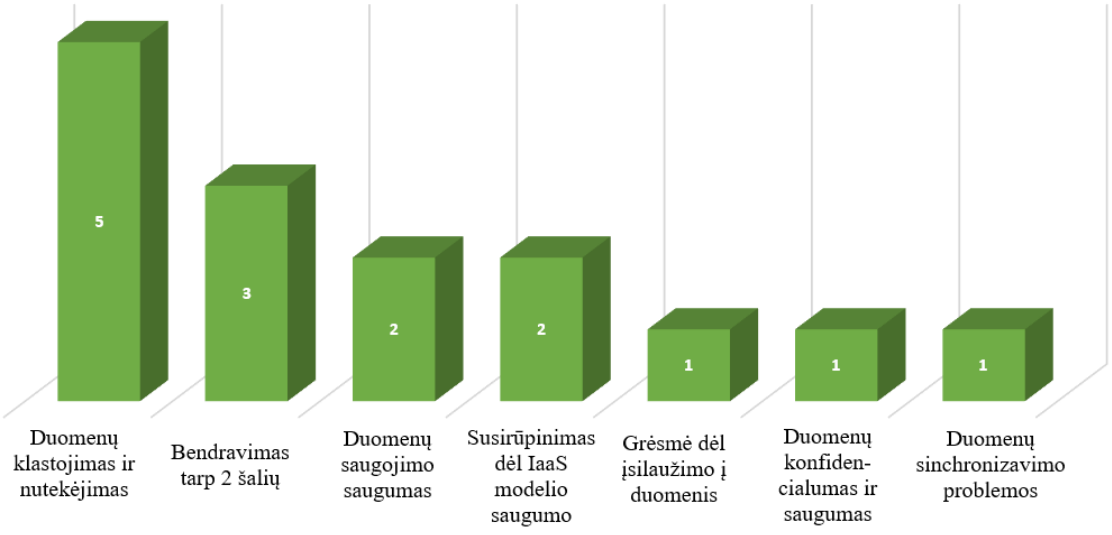
Šiandieninis gyvenimo tempas yra didžiausias per visą žmonijos istoriją. Tai kas buvo vakar- jau praeitis, o rytojus dar nenuspėjama ateitis, kurioje vieną iš svarbiausių vietų užima šiuolaikinės technologijos. Turbūt ne veltui nūdiena gali būti vadinama pokyčių ir revoliucijos laikmečiu. Pasauliui vis labiau skaitmeniškėjant, į elektroninę erdvę vis labiau persikelia ne tik piliečių tarpusavio bendravimas, įvairūs projektai, bet netgi darbas- tai ypač išpopuliarėjo 2020 metais dėka pasaulinės COVID-19 pandemijos. Sparčiai modernėjant kibernetinei aplinkai, augant verslo ir piliečių poreikiams, visoje Europoje ir pasaulyje viešojo administravimo modernizavimas tampa vis didesniu prioritetu. Tokia natūrali kaita ir interneto naudingumas bei reikšmingumas lėmė, kad iš viešasis valdymas vis labiau tobulėja ir keliasi į kibernetinę erdvę. Elektroninės valdžios atsiradimas buvo laikomas vienu reikšmingiausių pasaulinio tinklo pokyčių. Devintajame praeito šimtmečio dešimtmetyje, atsiradus pasauliniam tinklui, palaipsniui atsirado ne tik piliečių, bet ir valstybės valdymo organizacijų bei viešojo sektoriaus įstaigų poreikis daugiau paslaugų perkelti į internetą (Yadav ir Singh, 2012).

Suprasdama didėjančia kibernetinės erdvės svarbą, Indijos vyriausybė dar 1970 metais įsteigė Elektronikos departamentą (Butler ir kt., 2005). Vėliau sekė Nacionalinio informatikos centro įkūrimas 1977 metais. Šis įvykis buvo pirmasis didelis žingsnis Indijos elektroninės valdžios link, tačiau pagrindinį postūmį e. valdymui padarė 1987 m. pradėtas naudoti NIcNET – nacionalinis palydovinis kompiuterių tinklas (Butler ir kt., 2005). Dar vėliau buvo pradėta vykdyti Nacionalinio informatikos centro rajonų informacinės sistemos (DISNIc) programa/ Ši programa buvo skirta kompiuterizuoti visus rajonų (apygardų) biurus. Iki 1990 m. NIcNET buvo išplėstas per Indijos valstijų sostines iki visų rajonų būstinių (Butler ir kt., 2005). Elektroninės valdžios ivaldymą Indijoje pradėjo AHSHAYA projektas sukurtas Keralos valstijoje. Šio projekto mąstas buvo didelis, apėmė apie 5000 daugiafunkcinių bendruomenės technologijų centrų, vadinamųjų „Akshaya e-Kendra's“, visoje Indijos Keralos valstijoje. Šio projekto esmė ir pagrindinis siekis- mažinti gyventojų atskirtį, didinti elektroninių paslaugų prieinamumą ir patogumą, patenkinti gyventojų poreikius (Butler ir kt., 2005).

Ghaffar (2020) teigimu, e. valdžios institucijos pastaruoju metu daugiausia dėmesio skiria Informacijos ir Ryšių technologijų (IRT) sektoriaus plėtrai. Tai pasižymi tokių programų kaip vyriausybės debesų kompiuterija (angl. *Cloud Computing*), atvirojo kodo programos (angl. *Open Source programs*), dirbtinis intelektas (angl. *Artificial Intelligence*) ir panašiai. Pastarųjų metų tyrimai

parodė, kad vis daugiau vyriausybinių institucijų visame pasaulyje perėjo prie debesų kompiuterijos įvairiose valstybės valdymo institucijose ir sektoriuose. Manoma, kad tai galėjo lemti sėkmingos privataus sektoriaus patirtys (Ghaffar, 2020). Taip pat daugelis pasaulio šalių, siekdamos užtikrinti greitą ir sistemingą perėjimą prie debesų kompiuterijos, parengė atskiras strategijas. Pavyzdžiui, Suomija, Danija, Jungtinė Karalystė, Prancūzija, Japonija, Airija, Australija, Austrija, Vokietija, Honkongas, Japonija, JAE, Palestina, Egiptas ir kitos. Perėjimas prie debesų kompiuterijos valstybinėse įstaigose įgavo pagreitį, nes tikimasi didelių pranašumų institucijų perėjimo nuo tradicinių skaičiavimo metodų prie debesų kompiuterijos schemų (Ghaffar, 2020). Toks debesijos kompiuterijos pagreitis siejamas su didėjančiomis tarptautinėmis ekonominėmis krizėmis ir didėjančiais piliečių reikalavimais, todėl ypač didelis dėmesys skiriamas elektroninės valdžios plėtrai. Apskritai, debesų kompiuterija yra puikus sprendimas vyriausybėms, kurių internetinės svetainės patiria didžiulę apkrovą. Nors tai ir yra palygint nebrangus ir inovatyvus sprendimas, tačiau, kaip ir kiekviena nauja technologinė transformacija kelia susirūpinimą dėl kylančių kibernetinio saugumo užtikrinimo (Ghaffar, 2020).

2021 metais buvo atlikta sisteminė literatūros analizė, kurios tikslas apžvelgti esamus debesų kompiuterijos saugumo, grėsmių ir iššūkių mokslinius tyrimus. Analizės metu tyrėjai nagrinėjo 2010–2020 metais populiariose skaitmeninėse bibliotekose paskelbtus tyrimus (Tahirkheli ir kt., 2021). Tyrėjai išrinko 80 straipsnių, kurie atitiko pasirinktus kriterijus, t.y. būtų nagrinėjama ir aprašoma debesų kompiuterija, jos saugumas ir grėsmės jai. Dėka šios mokslinės literatūros analizės buvo išsiaiškintos septynios pagrindines debesų kompiuterijos paslaugų saugumo grėsmės (žr. 3 pav.).



3 pav. Debesų kompiuterijos saugumo grėsmės
Šaltinis: Tahirkheli ir kiti (2021)

Literatūros analizės rezultatai parodė, kad duomenų klastojimas ir nutekėjimas moksliniuose šaltiniuose buvo plačiausiai aprašyta problema ir kėlė didžiausią susirūpinimą tiek debesijos tiekėjams, tiek klientams. Tyrimas parodė, kad didelę grėsmę kelia duomenų saugojimo saugumas debesų kompiuterijos aplinkoje, kuomet netinkamai apsaugoti privatūs klientų duomenys gali būti neteisėtai panaudoti. Literatūros analizės rezultatai taip pat parodė, kad jautrių vartotojų duomenų perdavimas bei saugojimas išlieka iššūkiu tiek debesijos tiekėjams, tiek naudotojams (Tahirkheli ir kiti, 2021). Tyrėjų teigimu, debesų kompiuterijos vartotojai turi apsvarstyti galimas grėsmes jų duomenims prieš pradedant naudotis kompiuterijos paslaugomis. Taip pat tyrėjai siūlo klientams aktyviau naudotis blokų grandine (angl. *block chain*), kad saugumo užtikrinimas būtų efektyvesnis (Tahirkheli ir kiti, 2021).

Elektroninė valdžia ir debesų kompiuterija

Debesų kompiuterijos naudojimas tarp verslo ir gyventojų per pastarąjį dešimtmetį tikrai išsaugo, tačiau šiame magistro darbe noriu plačiau panagrinėti kaip debesų kompiuterijos naudojimas siejamas elektroninės valdžios koncepte. Fathey ir Odhman (2016) savo tiriamajame darbe aprašė debesų kompiuterijos taikymo naudas elektroninės valdžios portaluose:

1. **Diegimo paprastumas.** Viešojo sektoriaus organizacijos gali lengvai įdiegti debesų kompiuteriją, nereikia turėti sudėtingos aparatinės ar brangios programinės įrangos licenzijų (Liang, 2012).
2. **Kaštų taupymas.** Organizacijos gali sutaupyti ir sumažinti veiklos sąnaudas, mokėdamos tik už naudojamas paslaugas. Taip pat kadangi tam nereikia daug papildomo personalo sutaupomi kaštai skirti atlyginimams (Alshomrani, Qamar, 2013).
3. **Prieinamumas.** Debesų kompiuterija gali padidinti darbuotojų mobilumą, suteikdama prieigą prie informacijos ir paslaugų iš bet kurios vietos ir įvairių įrenginių (Liang, 2012).
4. **Ekologiškumas.** Debesų kompiuterija yra naudinga aplinkai, nes ji naudoja labai mažiau išteklių. Taigi, tai reikalauja daug mažiau energijos (Bansal ir kt, 2012).

Gartner (2018) atliktas tyrimas atskleidė, kad yra dvi pagrindinės kliūtys, apsunkinančios debesijos naudojimą viešajame sektoriuje- tai duomenų privatumas ir saugumas (van der Meulen, 2018). Tačiau debesijos kompiuterija geba atpažinti vartotojų elgesį, kad būtų išvengta galimo jautrių duomenų atskleidimo neįgaliotiems asmenims. Ypatingai jautrių duomenų klasifikavimas yra priemonė, kurią

vyriausybės gali naudoti norėdami parinkti tinkamiausią saugumo modelį skirtingoms duomenų kategorijoms pagal jų rizikos tolerancijos lygį (duomenų kritiškumą ar jautrumą) (Sun ir kt. 2014; Nur ir kt., 2022). Kita vertus, debesų kompiuterija, kaip ir kitos programos, susiduria su sunkumais.

Daugelis debesų kompiuterijos iššūkių elektroninės valdžios diegimui kyla dėl jos naujumo ir vis didėjančios plėtros. Fathey ir Odman (2016) susistemino šiuos sunkumus:

1. **Saugumo ir privatumo stoka.** Ypatingas dėmesys taikant debesų kompiuteriją turi būti skiriamas apdorojamų duomenų saugumui ir privatumui. Svarbu užtikrinti, kad ypatingos svarbos informacija būtų tinkamai saugoma.
2. **Veiklos tęstinumo trūkumas.** Didėjanti duomenų praradimo rizika dėl netinkamų atsarginių kopijų darymo arba sistemos gedimų yra už naudotojo įtakos ribos. Dėl to verslo tęstinumo užtikrinimas yra dar vienas iššūkis, į kurį reikia atkreipti dėmesį. Vyriausybės turi suprasti tęstinumo riziką ir būti užtikrintos, kad yra taikomos veiksmingos priemonės, pavyzdžiui, tvirtos sutartys, atstatymas po nelaimės ir veiklos tęstinumo planai, ypač jei naudojamos išorinės debesijos paslaugos. (Alshomrani ir Qamar, 2013).
3. **Priklausomumas nuo interneto.** Debesų kompiuterijos paslaugos yra visiškai priklausomos nuo interneto (Sahu ir Tiwari, 2012). Jeigu nėra galimybės prisijungti prie interneto ryšio, debesų kompiuterija nebegali veikti, o tai jau yra veiklos apribojimas, kuris daro kompiuteriją ne tokią patraukią ir ribojančią.
4. **Kiti papildomi iššūkiai.** Norint užtikrinti sklandų debesijos kompiuterijos naudojimąsi viešojo sektoriaus institucijose ir elektroninės valdžios portaluose susiduriama ir su kitais iššūkiais. Siekiant užtikrinti sklandų darbą, reikia atsižvelgti į augantį poreikį sukurti tinkamą strategiją, į taisyklių ir normatyvų bei politikos pataisas taip pat reikėtų atsižvelgti (Kundra, 2011).

Taigi, debesų kompiuterijos taikymas elektroninės valdžios sistemose ir portaluose yra naudingas, tačiau kaip visada vienareikšmiškai vertinti neišeina. Silpnosios debesų kompiuterijos grandys gali būti laikui bėgant patobulintos ir dar labiau pritaikytos naudoti ne tik verslo sektoriuje, bet ir viešajame valdyme. Daugelis debesų kompiuterijos iššūkių elektroninės valdžios diegimui kyla dėl jos naujumo ir vis didėjančios plėtros, todėl elektroninės valdžios portaluose naudojamą debesų kompiuteriją reikia kuo geriau adaptuoti būtent prie viešojo sektoriaus institucijų.

2. 2. Elektroninės valdžios sistemų įgyvendinimas Europoje

Europoje elektroninės valdžios strategijos sąvoka nėra palygint senas dalykas. 2018 metais Europos Sąjungoje buvo minimos 10 - osios elektroninės valdžios strategijos metinės (Europos Komisija, 2019). 2010 metais buvo paskelbta pirmoji elektroninės valdžios strategija. Jubiliejinėje dešimtmečio ataskaitoje buvo atskleista, kad nors Europos Sąjungos šalys skatinamos dirbti glaudžiai, tačiau jų kaip atskirų šalių kibernetinio saugumo klausimas ir brandumas vis tiek išlieka skirtingame lygmenyje (LR Seimo kanceliarija, 2021). Tokiam iš dalies panašiam, bet kartu ir skirtingam Europos Sąjungos valstybių narių viešojo valdymo sistemos susiformavimui didelės įtakos turėjo ir skirtingas valstybių kultūrinis, politinis ir istorinis kontekstas (LR Seimo kanceliarija, 2021). Europos Komisija ilgą laiką skatino šalis tobulinti savo elektroninės valdžios plėtrą, nes Europos šalių viešojo valdymo institucijos turi puikias galimybes pasinaudoti savanoriškomis priemonėmis skatinant elektroninės valdžios vystymąsi (Europos Komisija, 2019).

Dar 2006 metais Europos Komisija pripažino valstybių skaitmeninės transformacijos svarbą, kuomet priėmė vyriausybės veiksmų planą i2010. Tame veiksmų plane vienu iš svarbiausių aspektų buvo išskirtas klausimas kaip tenkinti visų gyventojų poreikius ir viešąsias paslaugas padaryti veiksmingesnes ir modernesnes (Europos Komisija, 2019). Europos viešojo administravimo institucijų pažangą diegiant e. vyriausybę ir sąveikumą nuo 2008 m. atidžiai stebi Europos Komisija, kasmet rengdama e. vyriausybės informacinius žiniaraščius, rengiamus pagal ISA2 programos Nacionalinės sąveikos sistemos observatoriją. Per 2008 - 2018 dešimtmetį e. vyriausybės informaciniuose lapuose buvo atskleistas pagrindinis viešojo administravimo reformų Europoje modernizavimas, išsamiai aprašant nacionalinius e. valdžios strategijų pokyčius, teisinę bazę, e. valdžios infrastruktūros plėtrą, skaitmeninių viešųjų paslaugų teikimą piliečiams ir įmonėms (Europos Komisija, 2019).

Naujausia ES kibernetinio saugumo strategija 2020 - 2025

Europos Komisija 2020 metais parengė naują ES kibernetinio saugumo strategiją. Strategijos laikotarpis: nuo 2020 m. iki 2025 m. ir orientuota į prioritetines sritis, kuriose ES gali padėti valstybėms narėms stiprinti visų Europoje gyvenančių asmenų saugumą, gerbdama mūsų vertybes ir principus. Europos Komisija reguliariai teikia ES saugumo sąjungos strategijos įgyvendinimo pažangos ataskaitas:

- Pirmoji pažangos ataskaita buvo pristatyta 2020 m. gruodžio 9 d.;
- Antroji ataskaita pristatyta 2021 m. birželio 23 d.;
- Trečioji ataskaita pristatyta 2021 m. gruodžio 8 d.;

- Ketvirtoji pažangos ataskaita buvo pristatyta 2022 m. gegužės 25 d.

Ketvirtojoje ataskaitoje pabrėžiamas Rusijos agresorės karas prieš Ukrainą. Šiuo karu ne tik keliama tiesioginė grėsmę Ukrainai, bet ir siekiama pakenkti pasauliniam stabilumui ir saugumui (Europos Komisija, 2022). Europos Sąjungos viduje tai kelia įvairių pavojų tiek piliečių saugumui, tiek energijos ir kitų žaliavų tiekimui. Šalys narės baiminasi, kad kibernetinės atakos gali būti nukreiptos prieš kritinės infrastruktūros objektus (Europos Komisija, 2022). Tačiau galime pasidžiaugti, kad naujų grėsmių akivaizdoje ES išliko ryžtinga ir vieninga. ES sustiprino budrumą bei šalių sienų apsaugos stebėseną. 2022 metų kovo 10–11 d. Versalio deklaracijoje Europos lyderiai pabrėžė būtinybę ruoštis greitai kylantiems iššūkiams, be kita ko, „apsaugoti save nuo nuolat augančio hibridinio karo, stiprinti mūsų kibernetinį atsparumą, apsaugoti mūsų infrastruktūrą, ypač svarbią infrastruktūrą, ir kovojant su dezinformacija“ (Europos Komisija, 2022).

Saugumo strategijoje nustatyti keturi pagrindiniai strateginiai ramsčiai ir toliau yra tiesiogiai susiję su šia užduotimi dabartinėmis geopolitinėmis aplinkybėmis:

1. Kurti patikimą kibernetinio saugumo aplinką;
2. Kovoti su besikeičiančiomis grėsmėmis;
3. Apsaugoti europiečius nuo terorizmo ir organizuoto nusikalstamumo; ir
4. Stiprinti Europos saugumo ekosistemą (Europos Komisija, 2022).

Taigi, net besikeičiant geopolitinėms aplinkybėms strategijos iškelti ramsčiai ir toliau yra svarbūs ir jų stiprinimo aktualumas tik didėja. Galime pasidžiaugti, kad net sunkiomis aplinkybėmis, Europos Sąjungos šalys yra stiprios ir vieningos ne tik Rusijos karo prieš Ukrainą klausimu, bet ir bendru saugios kibernetinės erdvės kūrimo aspektu.

Lietuvos Respublikos kibernetinio saugumo strategija

Lietuvos kibernetinio saugumo strategija buvo patvirtinta LR Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818. Strategijos pagrindinis tikslas: „Efektyviai ir laiku identifikuojant kibernetinius incidentus, užkertant kelią jų atsiradimui ir plitimui, valdant kibernetinių incidentų sukeltas pasekmes užtikrinti galimybę Lietuvos visuomenei saugiai naudotis informacinių ir ryšių technologijų (toliau – IRT) teikiamomis galimybėmis“ (Krašto apsaugos ministerija, 2018).

Kiti strategijos tikslai: stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą; užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą; skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą; stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą; stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą (Krašto apsaugos ministerija, 2018). Nenuostabu, kad lyginant Europos Sąjungos kibernetinio saugumo ir LR kibernetinio saugumo strategijas galima rasti daug panašumų. ES ir Šiaurės Atlanto sutarties organizacija (toliau – NATO) pripažįsta, kad kibernetinė erdvė pradedama naudoti kaip atskira karo erdvė arba kaip viena iš hibridinio karo priemonių (Krašto apsaugos ministerija, 2018). Žinoma, kad kibernetinėmis atakomis galima stipriai paveikti ypatingos svarbos valstybines infrastruktūras, pvz., 2010 m. įvykdyta kibernetinė ataka Irano branduolinės energetikos objekte; 2015 ir 2016 m. kibernetinės atakos Ukrainos elektros jėgainėse. Tokios ir panašios atakos gali neigiamai paveikti ne tik atskirų šalių, bet ir visos Sąjungos ekonominę ir socialinę gerovę. Pagal 2016 m. NATO viršūnių susitikimo Varšuvoje priimtą sprendimą dėl kibernetinės erdvės pripažinimo penktuoju kariavimo domenu Lietuvos kariuomenė tapo pagrindiniu Lietuvos Respublikos kibernetinės erdvės gynybos subjektu (Krašto apsaugos ministerija, 2018). Kibernetinio saugumo ir gynybos stiprinimas, efektyvus kibernetinių incidentų valdymas yra vienas iš svarbiausių veiksnių užtikrinant gyvybinius ir pirmaeilius valstybės nacionalinio saugumo interesus (Krašto apsaugos ministerija, 2018).

Taigi, naujausioje Lietuvos Respublikos kibernetinio saugumo strategijoje rašoma, kad nors pavieniai Lietuvos saugumo sričių rizikos vertinimo procesai jau yra pasiekę brandą, tačiau nacionaliniu lygiu saugumo rizikos vertinimo kultūra, kibernetinio saugumo rizikos vertinimas tebėra fragmentiškas. Trūksta kibernetinių grėsmių ir saugumo spragų analizės visapusės integracijos į veiklos rizikos vertinimo procesus, o sparčiai plėtojantis IRT už kibernetinį saugumą atsakingam personalui pradeda trūkti rizikos vertinimo žinių, gebėjimų ir praktikos. Todėl galima teigti, kad norint stiprinti Lietuvos kaip stiprios valstybės kibernetinio saugumo klausimu vaizdą reikia daugiau dėmesio skirti analizėms, atsakingo personalo žinių, gebėjimų didinimui ir tobulinimui.

2.3. Jungtinių Tautų šalių elektroninės valdžios raidos indeksas

Lengviausia pastebėti šalių tobulėjimą įgyvendinant elektroninę valdžią galima lyginant praeitį ir dabartį. Šiam tikslui įgyvendinti pasitelkti statistiniai duomenys, kurie išreikšti skaitine išraiška ir patalpinti į lentelę (žr. 1 lent.)

Nuo 2001 metų, Jungtinių Tautų Ekonomikos ir socialinių reikalų departamentas (UN DESA) kas dvejus metus skelbia EGDI (angl. *E-Government Development Index*)- Elektroninės valdžios raidos

indekso ataskaitą, kurioje dalyvauja 193 šalys. Per pastaruosius dešimt metų ši analizė įsitvirtino kaip pagrindinė elektroninės valdžios lyginamoji analizė, kuri naudinga ne tik piliečiams kaip edukacijos priemonė, bet ir politikams kaip palengvinamoji priemonė sprendimams priimti (Indijos Vyriausybė, 2022). Ši kas dvejus metus vykdoma apklausa yra vienintelė pasaulinė ataskaita, kurioje vertinama visų Jungtinių Tautų valstybių narių elektroninės valdžios raidos būklė. Analizėje vertinamas ir matuojamas šalių e. valdžios veiksmingumas viena kitos atžvilgiu, kas yra priešingybė konkrečiam šalies vertinimui. Ji pripažįsta, kad kiekviena šalis turi teisę nuspręsti kiek šiuo metu šaliai svarbus e. valdžios raidos indekso didinimas, remiantis nacionalinės svarbos aspektais (Indijos Vyriausybė, 2022). Apklausa daugiausia skirta politikos formuotojams, vyriausybės pareigūnams, akademinės bendruomenės, pilietinės visuomenės, privataus sektoriaus ir kitiems darnaus vystymosi, viešojo administravimo, skaitmeninės valdžios ir vystymuisi skirtų IRT sričių specialistams bei ekspertams (Indijos Vyriausybė, 2022).

1 lentelė. Šalių reitingavimas ir palyginimas pagal elektroninės valdžios raidos indeksą (angl. *EGDI*)

Vieta 2022 metais	Šalis	EGDI	Vieta 2018 metais	EGDI
1	Danija	0.9717	1	0.9150
2	Suomija	0.9533	6	0.8815
3	Pietų Korėja	0.9529	3	0.9010
4	Naujoji Zelandija	0.9432	8	0.8806
5	Islandija	0.9410	19	0.8316
5	Švedija	0.9410	5	0.8882
7	Australija	0.9405	2	0.9053
8	Estija	0.9393	16	0.8486
9	Nyderlandai	0.9384	13	0.8757
10	JAV	0.9151	11	0.8769
24	Lietuva	0.8745	40	0.7534

Šaltinis: Jungtinių Tautų e. valdžios plėtros duomenų bazė (2022).

Matematiškai EGDI yra vidurkis, kuris apskaičiuojamas pagal tris svarbiausius e. valdžios matmenis:

1. Internetinių paslaugų apimtį ir kokybę (angl. *Online Service Index,* OSI),
2. Telekomunikacijų infrastruktūros plėtros būklę (angl. *Telecommunication Infrastructure,* TII) ir
3. Žmogiškuosius išteklius (angl. *Human Capital Index,* HCI).

Kiekvienas iš šių indeksų yra sudėtinis matas, kurį galima išskirti ir analizuoti nepriklausomai, tačiau EGDI vidurkiui apskaičiuoti naudojama formulė:

$$EGDI = \frac{OSI + HII + HCI}{3}$$

Elektroninės valdžios raidos indekso analizė yra lyginamoji ir plėtros priemonė, skirta šalims mokytis vienai iš kitų, nustatyti stipriąsias sritis ir iššūkius e. vyriausybėje ir formuoti savo politiką bei strategijas šioje srityje.

Remiantis lentelės duomenimis, galima teigti, kad dauguma šalių, įskaitant ir Lietuvą, pajuto proveržį elektroninės valdžios vystymesi. Džiugu paminėti, kad iš išvardintų šalių didžiausią pokytį pajuto Lietuva (iš 40 pozicijos 2018 metais, 2022 metais pakilo net į 24 poziciją). Galime daryti prielaidą, kad Lietuvos Vyriausybė nusprendė dėti daugiau pastangų, remtis gerąja Europos bei pasaulio šalių praktika ir tobulinti e. valdžios vystymą. Taip pat džiugu, kad pirmaujančių šalių dešimtuke puikuojasi daug Europos Sąjungos šalių.

2.4. Elektroninės valdžios tobulinimas: Nacionalinio kibernetinio saugumo strategijos

Tačiau kaip ir viskas pasaulyje, taip ir valdžios bei visuomenės poreikiai smarkiai keičiasi ir norint sklandžiai vystyti viešąjį valdymą, reikalinga nuolat tobulinti e. valdžios sistemas ne tik ES, bet ir Lietuvoje. Kaip tobulėja kibernetinės atakos, taip pat ir elektroninių sistemų saugumas ir sklandaus darbo užtikrinimas tapo vis svarbesnis pasaulio valstybėms. Besikeičiančioms aplinkybėms ir didėjančios grėsmėms į pavojaus signalus valstybės į tokius įvykius kaip kibernetiniai nusikaltimai ėmė žiūrėti labai rimtai. Iš pradžių kai kurios šalys sukūrė ir priėmė kibernetinės gynybos reglamentus kaip nacionalinio saugumo strategijų dalį, vėliau akcentas buvo skiriamas vien tik kibernetinio saugumo strategijoms, o tai taip pat rodo perėjimą nuo kibernetinės gynybos prie kibernetinio saugumo koncepcijos (Patrascu, 2018).

Pirmąjį reikšmingą momentą kibernetinėje erdvėje, kuris sulaukė pasaulinio atgarsio, pažymėjo 2007 m. Estijoje įvykusi hibridinė ataka, kuri prasidėjo kaip riaušės dėl sovietinio laikmečio kario skulptūros perkėlimo iš Talino miesto centro į karių kapines, o baigėsi kibernetiniais išpuoliais (McGuinness, 2017). Iki atakų pradžios Estijos vyriausybės administracinę sistemą sudarė 150 viešųjų informacinių sistemų, aptarnaujančių apie 1000 elektroninių paslaugų. Apie puse Estijos piliečių naudojosi viešosiomis elektroninėmis paslaugomis, o įvairios organizacijos, valstybės valdymo organai

ir privačios įmonės Estijoje teikiamas skaitmeninėmis viešosiomis paslaugomis naudojosi kasdien (McGuinness, 2017; Patrascu, 2018). Bankinės operacijos daugiausia buvo elektroninės, kurios taip pat buvo orientuotos ir į provincijos gyventojus, kad būtų mažinama socialinė atskirtis tarp miesto ir kaimo gyventojų. Internetine balsavimo sistema pirmą kartą buvo galima pasinaudoti tose vietovėse, kuriose buvo prieiga prie tinklo (Patrascu, 2018). Palyginti su kitomis buvusiomis Rytų bloko šalimis, Estija tuo metu buvo daug labiau išsivysčiusi elektroninių viešųjų paslaugų tiekimo ir vykdymo klausimu – didelės investicijos į modernias technologijas ir gyventojų bei verslininkų susidomėjimas patraukliomis naujovėmis lėmė tokį spartų Estijos kaip lyderiaujančios skaitmeninės šalies augimą (Patrascu, 2018). Minėta kibernetinė ataka 2007 metais buvo vykdoma dviem skirtingais etapais. Pradžioje buvo vykdomi paprasti, spontaniški išpuoliai, pradėtos paslaugų atsisakymo (DOS) atakos prieš tikslinius kompiuterius, o po to – mirties atakos (PoD) (angl. *Ping of Death*), nukreiptos į vyriausybę ir Estijos spaudos svetaines (Patrascu, 2018). Antrajame etape atakos suintensyvėjo ir sudėtingėjo pradėdamos veikti per stiprius botnet tinklus. Tuo pačiu metu buvo užpultos kelios svarbios vyriausybinės svetainės. Šiame etape vyravo DDoS atakos, kurių poveikį pajuto ir vartotojai už šalies ribų (Patrascu, 2018). 2007 metais įvykusi ataka poveikį turėjo ne tik civiliams gyventojams (sutriko bankomatų, administracinių sistemų veikla), didžiausias neigiamas poveikis buvo vyriausybinėms organizacijoms, kurių darbuotojai ir tarnautojai negalėjo komunikuoti tarpusavyje, o žiniasklaidos priemonės negalėjo realiu laiku skelbi vykstančių naujienų (Patrascu, 2018).

Dar nuo 2005 metų Europos Komisija rengia ir priima veiksmų planus skirtus vykdyti viešojo sektoriaus modernizavimą Europos Sąjungoje. Šiais veiksmų planais siekiama bendrumo Europos veiklos koordinavimui, bendradarbiavimui ir jungtiniams veiksmams e. valdžios srityje (Europos Komisija, 2016). Europos Komisijos Veiksmų planas buvo parengtas ir pristatytas 2016 metų liepos mėnesį. Naujausias planas parengtas 2021-2027 metų laikotarpiui ir yra skirtas integracijai ir įtraukčiai. Naujausiu planu skatinamos vietinių organizacijų, pilietinių bendruomenių iniciatyvos ir remiamos gerosios šalių narių praktikos (Europos Komisija, 2020). 2021-2027 m. Veiksmų planas remiasi 2016 metų plano principais ir tikslais, tačiau naujajame plane daugiau dėmesio skiriama ne tik asmenų iš trečiųjų (ne Europos Sąjungos) šalių, bet ir migrantų kilmės ES piliečių integracijai.

Bendra e. valdžios pažanga, įgyvendinant veiksmų planą, turėtų būti vertinama kasmet, taikant įvairius vertinimo būdus ir metodus: lyginamąją analizę, mokymąsi remiantis patirtimi, individualios veiklos vertinimą, viešųjų duomenų analizę, vartotojų lūkesčius ir kt. Kad suinteresuotosios šalys galėtų plėtoti bendras vertinimo procedūras, valstybės narės su Europos Komisija ir kitomis valstybėmis narėmis turėtų dalintis atitinkamų iniciatyvų atliktų tyrimų lyginamosios analizės rezultatais.

2.4.1. Atvejo analizė: Danijos Karalystė

Dar palyginti neseniai šalis, kurios gyventojų skaičius nesiekia 6 milijonų, buvo kibernetiškai stiprių šalių, tokių kaip Jungtinės Amerikos Valstijos, Izraelis ar Jungtinė Karalystė šešėlyje. Tačiau Danijos vyriausybė išsikėlė tikslą maksimaliai tobulinti šalies kibernetinį saugumą bei elektroninės valdžios raidos indeksą.

2021 metais Užsienio reikalų ministerija paskelbė, kad pagal Didžiosios Britanijos saugumo tyrimų įmonės „Comparitech“ duomenis Danija užėmė pirmąją vietą tarp kibernetinių saugumo priemonių pasaulyje su 3,56 balo vidurkiu. Kyla klausimas kaip Danijai taip pavyko? (Venkina, 2021). Toks spartus šalies kibernetinio saugumo augimas gali būti siejamas su 2016 metais JAV įvykusia kibernetine ataka, kurią surengė programišių grupė, žinoma kaip APT28 arba dar kitaip “Fancy Bear”, kuri yra glaudžiai siejama su Rusijos karine žvalgyba. Ataka buvo nukreipta į JAV Demokratų partijos serverius, kurių dėka programišiai gavo prieigą prie „atrinktų Danijos gynybos narių el. pašto paskyrų“ (Venkina, 2021). Nors nutekinti duomenys buvo apibūdinami kaip neįslaptinti, jie galėjo būti panaudoti darbuotojų šantažavimui. Tuometinis Danijos gynybos ministras Clausas Hjortas Frederiksenas šį pažeidimą įvertino kaip „labai kritinę situaciją (Venkina, 2021). Dabar, praėjus kuriam laikui po atakos išaiškinimo, Danija yra „Comparitech“ reitingo viršūnėje kaip pirmaujanti šalis kibernetinio saugumo kontekste.

Kaspersky Lab atlikto tyrimo 2020 metų III ketvirčio duomenys rodo, kad danai yra ypač stipriai apsisaugoję savo asmeninius duomenis, domisi skaitmenine higiena ir turi gerą suvokimą apie kibernetinį saugumą. Pastarąjį bent iš dalies lemia plačiai paplitęs dviejų veiksnių autentifikavimas. Tai nesudėtingas, bet efektyvus būdas blokuoti atakų vektorius atsižvelgiant, kad skaitmeniniai parašai naudojami norint prisijungti ne tik prie prie asmeninių paskyrų, bet ir prie visų vyriausybinių internetinių paslaugų finansų sektoriuje (Venkina, 2021).

Nors Danija ir yra viena iš atspariausių šalių prieš kibernetines atakas, nereiškia, kad šalies ar jos gyventojų atakos visiškai nepasiekia. Prieš investuojant gausybę lėšų ir laiko, Danija buvo viena iš reguliariai hakerių atakuojamų šalių. Štai keletas ryškiausių kibernetinių atakų per paskutinius metus:

2020 m. vasarį buvo pažeistas Danijos mokesčių portalas ir nutekinta 1,26 mln. danų, t.y. penktadalio visų šalies gyventojų, asmens duomenys. Nutekėjus buvo CPR numeriai, naudojami banko sąskaitoms nustatyti, telefonų numeriams gauti ar kitoms svarbioms užduotims atlikti, ir įvyko dėl programinės įrangos klaidos. 2020 m. Danijos nacionalinį banką ištiko „SolarWind“ ataka. Šiuo atveju

įsilaužėliai septynis mėnesius naudojosi “užpakalinėmis durimis” (angl. *Back door*) į Nacionalinį banką, kol įsibrovimą pastebėjo amerikiečių įmonė (Chebac, 2022).

Dar viena ataka buvo įvykdyta 2020 m. Tuomet išpirkos reikalaujanti (angl. *Ransomware)* ataka. Ši ataka buvo didelio mąsto ir paveikė ketvirtadalį Danijos naujienų agentūrų. Viena didžiausių naujienų agentūrų šalyje Ritzau. Agentūra visiškai užsidarė dviem dienoms, todėl jos 10 milijonų radijo klausytojų, 8 milijonai televizijos žiūrovų, 15 milijonų skaitytojų pasikliovė tik tiesioginiais (angl. *Live blogging*) įrašais iš pačių darbuotojų paskyrų (Chebac, 2022). Didžiausia pasaulyje vėjo turbinų gamintoja „Vestas“ 2021 m. tapo didžiulės kibernetinės atakos auka. Dėl atakos buvo prarasti daugybę privačių duomenų, ypač darbuotojų ir partnerių asmeniniai duomenų. Nutekinta informacija apėmė vardus, pavardės, kontaktinę informaciją, tokią kaip gyvenamosios vietos adresai, el. pašto adresai, telefonų numeriai, išsilavinimas, profesiniai įgūdžiai, nuotraukos ir išsami informacija apie darbo prašymus bei CV. Tai buvo didžiulis smūgis bendrovės prekės ženklui ir jos akcijų vertei, kuri sumažėjo 6% (Chebac, 2022).

Ekspertai teigia, kad Danijos kibernetinio saugumo centrams buvo pranešta 2017 metų balandį, kai buvo atskleista, kad įsilaužėliams pavyko pasiekti Danijos gynybos narių el. paštus. Manoma, kad šis išpuolis buvo atspirties taškas Danijos karalystės kibernetinio saugumo ir elektroninės valdžios stiprinimui.

Elektroninė valdžia Danijos Karalystėje

Danija vertinama kaip viena stipriausių valstybių kalbant apie viešojo sektoriaus skaitmeninimą. Su vienu skaitmeniniu raktu galite saugiai pasiekti daugiau nei šimtą skirtingų viešųjų paslaugų ir, be to, įvairių privačių paslaugų. Tai palengvina piliečių kasdienybę ir įvairias jiems reikalingas paslaugas padaro lengvai prieinamas – nuo vaikų registravimo į darželį iki sąskaitų apmokėjimo per elektroninę bankininkystę (Danijos užsienio reikalų ministerija, 2022). Kiekvienas pilnametis Danijos pilietis gali turėti saugų skaitmeninį raktą, daniškai vadinamą „NemID“ arba angliškai „Easy-ID“. Šis raktas yra skirtas bei naudojamas viešosioms skaitmeninėms paslaugoms pasiekti ir užsisakyti viešajame ir privačiame sektoriuose. Danijos e. valdžios strategijoje nustatyta, kad nuo 2013 metų valstybinės institucijos Danijos įmonėms laiškus siųs tik elektroniniu būdu, o nuo 2015 metų įmonės privalomai turi reikalingas ataskaitas institucijoms pateikti skaitmeniniu būdu. Visos Danijos šalies įmonių ataskaitos skirtos valdžios institucijoms bus teikiamos vienoje vietoje- interneto svetainėje www.borger.dk (Skaitmeninės valdžios agentūra).

Danija nuolat stiprina savo šalies kibernetinį saugumą ir nuėjo ilgą kelią, kad jau kelerius metus, 2019, 2020 ir 2021 m., būtų pripažinta saugiausia valstybe pasaulyje kibernetinio saugumo aspektu (Chebac, 2022).

Priemonės padedančios Danijos Karalystei pirmauti kibernetinio saugume:

- Dviejų veiksnių autentifikavimas- dažniausiai naudojamas vyriausybinėse tarnybose ir finansinėse programose;
- Labai stiprios ir gerai išvystytos bankininkystės programėlės.
- Didelės investicijos į kibernetinį ir informacijos saugumą;
- Nuosekli kibernetinė politika, pagrįsta: didėjančiu technologiniu atsparumu, piliečių žinių gerinimu ir įvairių veikėjų veiklos koordinavimu;
- Aktyvus darbas su valstybinės svarbos infrastruktūromis;
- Visą parą veikiančio situacijų centro kūrimas;
- Programėlės „Mano skaitmeninė savisauga“ (dan. *Mit digitale selvforsvar*) paleidimas. Programėlėje pateikiama informacija apie skaitmeninius sukčiavimus, virusų ir kenkėjiškų programų atakas, ir netgi konkretūs patarimai ką reikėtų daryti, jei įvyktų pažeidimas (Chebac, 2022).

Tačiau reikia nepamiršti, kad nors Danija kurį laiką ir yra viena pirmaujančių šalių kibernetinio saugumo kontekste, vis dėl to, skirtingai nei pavyzdžiui JAV, Danija nėra suvokiama kaip aukšto lygio kibernetinis taikinys (Venkina, 2021). Nors, 2021 m. birželio mėnesio CFCS vertinimu, kibernetinio šnipinėjimo ir elektroninių nusikaltimų grėsmės lygis Danijoje buvo labai aukštas, destruktyvių kibernetinių atakų prieš Danijos valdžios institucijas ir privačias įmones grėsmė išlieka maža. Tai reiškia, kad didelio mąsto ataka prieš Danijos Vyriausybę artimiausiu metu yra mažai tikėtina.

Lietuva dėka geopolitinių aplinkybių, lokacijos ir agresyvių šalių kaimynių tokia rami kaip Danija galbūt ir negali būti, bet gali iš Danijos Karalystės pasisemti gerosios praktikos stiprinant šalies elektroninį valdymą bei kibernetinį saugumą. Viena naudingiausių inovacijų Lietuvai būtų skaitmeninės programėlės „Mano skaitmeninė savisauga“ įdiegimas ir paleidimas. Piliečių, vartotojų bei viešojo sektoriaus švietimas kibernetinio saugumo klausimu didinimas bei aktyvus darbas su valstybinėmis institucijomis Lietuvai būtų puikus kelias link kibernetiškai stiprios valstybės vardo.

2.4.2. Atvejo analizė: Naujoji Zelandija

Naujoji Zelandija (NZ) kaip šalis, kurios geroji praktika praverstų Lietuvai taip pat pasirinkta neatsitiktinai. Darbo autorės nuomone, kad šalių gerąja praktika būtų galima pasinaudoti operatyviai, šalys turi būti kiek įmanoma panašesnės. Gyvais Worlmeter duomenimis (2022), Naujoje Zelandijoje 2022 metų lapkritį buvo 4,9 mln gyventojų, o Lietuvoje 2,7 mln. Žinoma, skaičiai skiriasi, bet jeigu žvelgsime į bendrą gyventojų populiaciją pagal šalis, skirtumas nebus toks didelis- Zelandija užima 126 vietą tarp visų šalių, o Lietuva yra 142 vietoje iš 235 šalių.

Naujoji Zelandija rodo gerą pavyzdį ir remiantis duomenimis (žr. 2 lent.) yra pirmaujančių šalių dešimtuke pagal elektroninės valdžios raidos indeksą. Kas rodo, kad šalis tobulina savo strategiją, veiksmų planą ir elektroninės valdžios raidos gerinimas yra vienas iš svarbiausių aspektų šaliai. Nacionalinio kibernetinio saugumo centras Naujoje Zelandijoje yra Vyriausybės ryšių apsaugos biuro dalis (pradėjo veikti dar 1977 metais, tačiau 2003 metais buvo modernizuota). Nacionalinis kibernetinio saugumo centras buvo paleistas 2011 metais.

Nuo tada centro pareigos yra:

- Teikti pažangias kibernetinių grėsmių aptikimo ir trikdymo (CORTEX) kibernetinės apsaugos rekomendacijas ir pasiūlymus;
- Reaguoti į didelio poveikio kibernetinius incidentus nacionaliniu lygmeniu;
- Tvarkyti Naujosios Zelandijos vyriausybės informacijos saugumo standartus; ir
- Rengti ataskaitas apie kibernetines grėsmes šalyje (Barker, 2021).

Naujosios Zelandijos Nacionalinio kibernetinio saugumo centras (angl. *NCSC*) vykdo kenkėjiškų programų aptikimo ir trikdymo paslaugą, kuri yra vadinamą Cortex. „Cortex“ vidinė veikla įslaptinta, tačiau ji naudoja įvairių šaltinių grėsmės žvalgybą, kad apsaugotų tam tikrą Naujosios Zelandijos organizacijų grupę. 2018 m. „Cortex“ laimėjo du apdovanojimus. „iSANZ“ apdovanojimuose- „Cortex“ kaip geriausias saugumo projektas, o Viešasis Naujosios Zelandijos administravimo institutas (IPANZ) pripažino „Cortex“ kompetencijos apdovanojimu už patikimą vyriausybės kūrimą (Barker, 2021).

Elektroninė valdžia Naujojoje Zelandijoje

Naujoji Zelandija vyriausybės funkcijoms gerinti naudoja skaitmenines technologijas nuo 1996 m., o internetinės paslaugos teikiamos nuo 2000 metų. Šalis buvo viena iš pirmųjų, pakeitusi popierines formas ir dokumentus ir pradėjusi naudoti elektroninius dokumentus ir elektronines formas, taip pat elektroninį atsiskaitymą bei prieigą prie skaitmeninių įrašų (Sear, 2021). Naujoji Zelandija parodė gerą

pavyzdį, kaip įdiegti ir pritaikyti skaitmenines naujoves vyriausybėje. Per 2016 m. vasaros olimpines žaidynes šalis tapo mobiliojo bilietų pardavimo pradininke taip pat viena pirmųjų šalių pasaulyje kuriant mobilią infrastruktūrą. Štai keletas skaitmeninių naujovių, kurias šalis įdiegė arba planuoja įgyvendinti:

- **Skaitmeninė valdžia ir privatumas.** Naujosios Zelandijos vyriausybė skaidriai žiūri skaitmenines operacijas, įskaitant piliečių duomenų rinkimą ir naudojimą. Naudodama privatumo valdymo sistemą Naujoji Zelandija parodo, kaip vertina skaidrumą vyriausybinėse agentūrose, bendraudama su piliečiais tokiomis svarbiomis temomis kaip asmens duomenų apsauga.
- **Skaitmeninės tapatybės programa.** Programa apima bendradarbiavimą, tyrimus su pagrindiniais skaitmeninės tapatybės ekosistemos dalyviais. Privatus ir viešasis sektorius perkelia daugiau paslaugų į interneto erdvę, todėl žmonės tikisi, kad galės naudotis paslaugomis ir atlikti sandorius nuotoliniu būdu, greitai, saugiai ir be popierinių dokumentų. Ši programa užtikrina aukštą vartotojo asmeninės informacijos saugumo lygį.
- **Skaitmeninių paslaugų teikimas.** NZ vyriausybė daugiausia dėmesio skyrė efektyvumo didinimui, skaidrumo didinimui ir pagalbos teikimui klientams. Pagrindinis tikslas – sukurti racionalesnį požiūrį į skaitmeninių paslaugų teikimą, kuris užtikrintų pažangą visuose sektoriuose, įskaitant verslą, švietimą, socialines paslaugas, visuomenės saugumą ir informacines technologijas. Štai kodėl Vyriausybė pristatė Skaitmeninės viešosios paslaugos strategiją, kurioje nurodoma viešųjų paslaugų modernizavimo kryptis, valstybės tarnybų centre iškeliant žmones ir verslą (Sear, 2021).

Pagrindinis Naujosios Zelandijos veiksmų plano tikslas– tobulinti nacionalinę Kompiuterinę avarijų likvidavimo komandą (CERT), kuri sumažintų kibernetinių incidentų žalą bei pagerintų šalies gebėjimą susidoroti su šiomis atakomis. CERT yra kaip vienas prieigos taškas visoms organizacijoms ar asmenims, kuriems reikia pagalbos, ir teiks informaciją įvairaus dydžio įmonėms, vyriausybei ir asmenims, kad jie galėtų apsisaugoti nuo kibernetinių nusikaltėlių (Sear, 2021).

Naujosios Zelandijos vyriausybės ryšių ministras Amy Adams yra pasakęs, kad „Pokyčių tempas ir naujų bei sudėtingų grėsmių atsiradimas reiškia, kad reikia nuolatinio budrumo. Kasmet atnaujindami veiksmų planą, neatsiliksime nuo bet kokios kylančios grėsmės“. Manau tokia mintis labai tinka ir Lietuvai siekiant tapti kibernetiškai stipria valstybe. Nuolatinis veiksmų plano tobulinimas ir įgyvendinimas yra vienas iš būdų kaip tapti būtent tokia valstybe.

Taigi, apibendrinant šių dviejų valstybių pavyzdžius galima teigti, kad norint jog valstybė taptų kibernetiškai saugesnė, o jos elektroninė valdžia būtų stipresnė, reikia šiuos du punktus padaryti vienais

iš prioritetinių. Prioritetinėms sritims yra skiriamas didesnis finansavimas, todėl valstybei svarbios sritys gali būti labiau išvystytos ir patobulintos.

2.5. Lyginamoji analizė: Lietuvos situacija pasaulio ir Europos Sąjungos elektroninės valdžios kontekste

Nenuostabu, kad nors ir Europos Sąjungą sudaro 27 valstybės narės, visų jų ekonomikos, politikos, viešojo sektoriaus valdymas ir struktūra bei rezultatai yra skirtingi. Lietuva dažnai linksniuojama kaip viena iš atsiliekančių šalių bendrame ES kontekste, tačiau, mano nuomone, verta atkreipti dėmesį į tas sritis, kuriose Lietuva pirmauja.

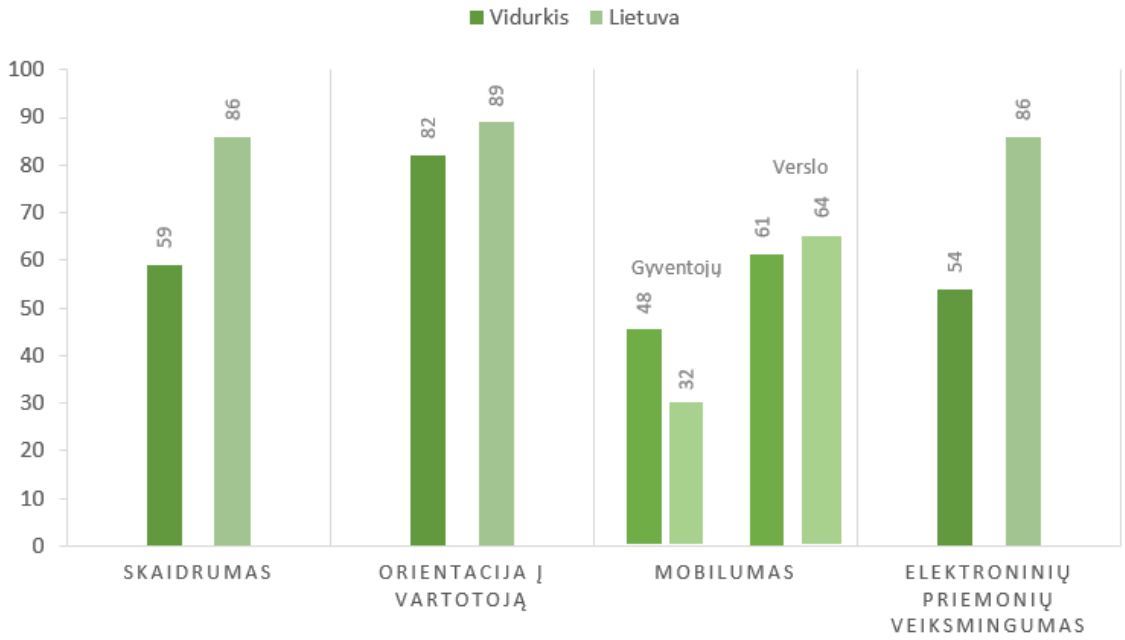
2018 metais Europos Komisija užsakė tyrimą, kuris parodė, kad 10 Europos Sąjungos šalių (Malta, Austrija, Švedija, Suomija, Nyderlandai, Estija, Lietuva, Latvija, Portugalija, Danija) ir Norvegija teikia aukštos kokybės skaitmenines paslaugas, kurių balas viršija 75 %. Aktyviai plečiant viešąsias elektronines paslaugas, gyventojams palengvinamas kasdienis gyvenimas, pavyzdžiui, darbo susiradimas, naujo verslo kūrimas, studijų pradėjimas ir pan. Šalys, kurių skaitmeninis našumas buvo mažesnis turi tikslą vytis ir lygiuotis į pirmaujančias šalis, mažinti atotrūkį, siekdamos įgyvendinti Europos tikslą sukurti bendrą skaitmeninę rinką. Galime pasidžiaugti, kad lyginant elektroninėje erdvėje teikiamų paslaugų pasiekiamumą ir pačios elektroninės valdžios integraciją į visuomenę, Lietuva vertinama kaip viena iš perspektyviausių valstybių Europoje (Europos Komisija, 2018)

Tyrimas ir vertinimas buvo atliekamas 34-ose valstybėse: ES valstybėse narėse, bei Šveicarijoje, Juodkalnijoje, Serbijoje, Turkijoje, Islandijoje ir Norvegijoje.

Tyrimo kokybei užtikrinti pasirinkti keturi pagrindiniai kriterijai, pagal kuriuos šalys buvo lyginamos ir vertinamos:

- Skaidrumas,
- Orientacija į vartotoją,
- Mobilumas,
- Elektroninių priemonių (dokumentų) veiksmingumas.

Pagal pagrindinius atlikto tyrimo vertinimo kriterijus buvo sudaryta diagrama (žr. 4 pav.), kurioje pateikiama informacija: tyrime dalyvavusių 34 šalių vidurkis bei Lietuvos statistika. Duomenys pateikiami procentine išraiška.



4 pav. Tyrimo duomenys stulpelinės diagramos išraiška
Šaltinis: Europos Komisija (2018)

Skaidrumas- šis rodiklis parodo, kiek šalių vyriausybės yra skaidrios viešųjų paslaugų teikimo procese, kuris yra vykdomas elektroninėje erdvėje, taip pat viešųjų organizacijų atsakomybę ir ivartotojų galimybės kontroliuoti jų asmeninius duomenis lygį. Šio kriterijaus bendras ES valstybių narių vidurkis - 59 %, Lietuvos - 86 %.

Orientacija į vartotoją- šis kriterijus nurodo višųjų paslaugų mastą, kurios teikiamos internetinėje erdvėje, taip pat jų pritaikymą mobiliems telefonams. Orientacija į vartotoją yra labiausiai išvystytas elektroninės valdžios požymis. Šio kriterijaus bendras ES valstybių narių vidurkis – 82 %, tuo tarpu Lietuvoje šis rodiklis 89 %.

Mobilumas (tarpvalstybinis judrumas) - šiuo kriterijumi nurodoma kiek plačiai žmonės gali naudotis viešosiomis paslaugomis už savo šalies ribų). Šio kriterijaus bendras ES valstybių narių vidurkis – 52 %. Lietuvos kriterijaus reikšmė pateikiama dviem aspektais: gyventojų judumas - 32 % (ES vidurkis - 48 %), verslo judumas - 64 % (ES vidurkis - 61 %).

Elektroninių priemonių veiksmingumas (eID, e. dokumentas, e. pristatymas ir kita) - nurodo kiek ir kokios sąlygos yra sudarytos elektroninėms paslaugoms teikti, pvz.: elektroninis identifikavimas ir autentiški šaltiniai. Šio kriterijaus bendras ES valstybių narių vidurkis - 54 %, Lietuvos – 86 %.

Taigi, Europos Komisijos paskelbtos elektroninės valdžios veiksmingumo ataskaitos duomenimis, Lietuvos bendras indeksas 2016 - 2017 m. laikotarpiu buvo didesnis negu 75 % (Europos Komisija,

2018). Apibendrinant galima teigti, kad Lietuva tikrai savo šalies skaitmeninimą iškelia kaip prioritetinę sritį ir galime pasidžiaugti jog lyginant su 34- ių šalių vidurkiu beveik visose grafose esame aukščiau jo. Dėka tyrimo išsiaiškinta, kad Lietuvoje būtų galima pagerinti gyventojų ir verslo judrumą, kad būtų pasiektas didesnis gyventojų mobilumas ir tarpvalstybinis judrumas.

3. KIBERNETINIO SAUGUMO UŽTIKRINIMAS

3.1. Kibernetinio saugumo architektūra Lietuvoje

Tam , kad geriau suprastume kaip veikia kibernetinio saugumo užtikrinimas Lietuvoje, turime žinoti architektūrą (žr. 5 pav.)

Architektūros piramidės viršuje yra **LR Vyriausybė**, kuri nubrėžia Lietuvos kibernetinio saugumo politikos gaires, pavyzdžiui, tvirtindama ilgalaikius planus ar programas. Žemiau yra **Krašto apsaugos ministerija** ir **Kibernetinio saugumo taryba**. Krašto apsaugos ministerija rengia Kibernetinio saugumo sritį reguliuojančius teisės aktus, pavyzdžiui, Kibernetinio saugumo įstatymą. Ministerijai savo rekomendacijomis ir pasiūlymais padeda Kibernetinio saugumo taryba, sudaryta iš mokslo, viešojo ir privataus sektorių atstovų (LR KAM, 2022).

Krašto apsaugos ministerijos parengtų teisės aktų įgyvendinimą užtikrina **Nacionalinis kibernetinio saugumo centras** (atsakingas už kibernetinių incidentų valdymą visoje Lietuvoje), **Lietuvos policija** (atsakinga už kibernetinių nusikaltimų užkardymą, tyrimą ir prevenciją) ir **Valstybinė duomenų apsaugos inspekcija** (tiria kibernetinius incidentus, susijusius su asmens duomenų pažeidimais). Šios institucijos bendradarbiauja ir dalijasi informacija apie kibernetinių incidentų tendencijas ir grėsmes (LR KAM, 2022).

Kibernetinio saugumo subjektai yra Lietuvoje veikiančios valstybės institucijos ir privačios organizacijos. Jos privalo įgyvendinti kibernetinio saugumo teisės aktų reikalavimus, pavyzdžiui, periodiškai atlikti savo tvarkomų informacinių sistemų rizikos vertinimą, pasitvirtinti kibernetinio saugumo politikos ir jos įgyvendinimo dokumentus, įgyvendinti atitinkamas technines saugumo priemones. Administracinių nusižengimų kodekse yra įtvirtintos baudos už nustatytų kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, nevykdymą (LR KAM, 2022).

5 pav. Kibernetinio saugumo architektūra Lietuvoje
Šaltinis: LR Krašto apsaugos ministerija (2022)

Spalio mėnesis Lietuvoje dar kitaip vadinamas Kibernetinio saugumo mėnesiu. 2022 metų spalio 18 d. prasidėjo pagrindinės ir didžiausios šiais metais nacionalinės kibernetinio saugumo pratybos pavadinimu „Kibernetinis skydas 2022“. Jose savo kibernetinio saugumo žinias ir gebėjimus reaguoti į įvairaus tipo kibernetines grėsmes tikrinosi daugiau nei 110 organizacijų. Tai yra didžiausias dalyvių skaičius per visą šių pratybų organizavimo istoriją (LR KAM, 2022). Krašto apsaugos viceministro Margirio Abukevičiaus teigimu, šių metų vasarą įvykę kibernetiniai išpuoliai Lietuvoje ir karas Ukrainoje įtikino, kad kibernetinio saugumo grėsmės yra realios. Taip pat viceministro teigimu didelis dalyvių skaičius rodo, kad organizacijos vis labiau iškelia kibernetinio saugumo klausimą kaip vieną pagrindinių (LR KAM, 2022). Didžiausią dalyvių skaičių sudarė subjektai iš viešojo ir privataus sektorių, kurie Lietuvoje yra atsakingi už valstybės informacinius išteklius, ypatingos svarbos informacinę infrastruktūrą, viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų teikimą. Pratybose taip pat dalyvavo Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, Valstybinė duomenų apsaugos inspekcija ir Lietuvos policija (LR KAM, 2022).

Šių pratybų „Kibernetinis skydas 2022“ vadovas pulkininkas Romualdas Petkevičius teigia: „Šiais metais pratybų dalyviams pasiūlėme dvi naujoves – tai kibernetinio sukčiavimo (angl. *Phishing*)

imitavimo įrankį ir galimybę kibernetinius incidentus tirti pasinaudojus šią vasarą pradėjusiu veikti NKSC virtualiu kibernetinio saugumo poligonu (angl. *Cyber Range*)“ (LR KAM, 2022).

Tokios pratybos dalyvavusiems jose suteikė dar daugiau naudos, nes kaip žinia, didėjančios kibernetinio saugumo grėsmės dažnai lenkia praktinį saugumo įgyvendinimą, todėl svarbu neatsilikti. 2020 metais spalio mėnesį vykusių pratybų metu virtualaus kibernetinio saugumo poligono galimybes išbandė 16 dalyvių, o Phishing’o įrankį virš 90 organizacijų. Pratybas „Kibernetinis skydas 2022“ organizavo Lietuvos Regioninis kibernetinės gynybos centras (NKSC filialas), Kauno technologijos universitetas ir LITNET techninis centras (LR KAM, 2022). Šios pratybos vyko ir LR Prokuratūroje. Darbuotojams į jų darbinius elektroninius paštus buvo siunčiamos sukčiavimo imitavimo žinutės. Iš viso žinutės buvo siųstos 1048 prokuratūros darbuotojams.

Spalio 17 d. buvo išsiųsta žinutė apie netikėtai "nežinia iš kur" gautą siuntą Ją perskaitė 305 darbuotojai, iš jų 168 nuspaudė nuorodą į nepatikimą svetainę, 63 darbuotojai suvedė prašomus asmens duomenis, kuriuos piktavaliai pasisavino.

Spalio 18 d. žinutes tariamai siuntė Tyrimai.lt noreply@tyrimai.it. Gautą žinutę atsidarė ir perskaitė 172 prokuratūros darbuotojai, iš jų 91 susiviliojo ir nuspaudė žalingą nuorodą, 56 darbuotojai suvedė ir pasidalino savo asmenine informacija su piktavaliais. Tą pačią dieną tariamai laišką siuntė ir SoDra noreply@sodra.it. 170 žinutės gavėjų atsidarė el. laišką, iš jų 76 nuspaudė žalingą nuorodą, 45 žinutę gavę darbuotojai suvedė asmeninę informaciją.

Spalio 19 d. Apsimestinius laiškus siuntė Epolicija noreply@epolicija.it. Gautą žinutę perskaitė 243 darbuotojai, iš jų klaidinančią nuorodą į nepatikimą svetainę spustelėjo 175, o 102 darbuotojai suvedė ir pasidalino savo asmens duomenimis su piktavaliais. Į piktavalių suregztas pinkles įkliuvo 16,7 proc. darbuotojų. Manoma, kad šį laišką ir nuorodas spaudė daugiau darbuotojų, nes policija yra ta institucija, su kuria prokuratūros darbuotojai glaudžiai bendradarbiauja. Todėl daugumai tai nesukėlė įtarimų ir į gautą informaciją darbuotojai pažiūrėjo neatidžiai. Tą pačia dieną apsimestines žinutes siuntė ir Mano VMI noreply@vrni.it. Gautą žinutę perskaitė 72 darbuotojai, iš jų 7 nuspaudė žalingą nuorodą, viena darbuotoja pateikė asmeninę informaciją, įskaitant asmens kodą.

Spalio 20 d. laiškus tariamai siuntė Epaslaugos noreply@epaslaugos.it. Gautą žinutę perskaitė 55, iš jų 10 darbuotojų nuspaudė žalingą nuorodą, 5 darbuotojai pateikė asmeninę informaciją piktavaliams.

Mažėjantis darbuotojų susidomėjimas gaunamais el. laiškais rodo, kad jie tapo budresni ir prieš spaudžiant aktyvias nuorodas įdėmiau pasiskaito.

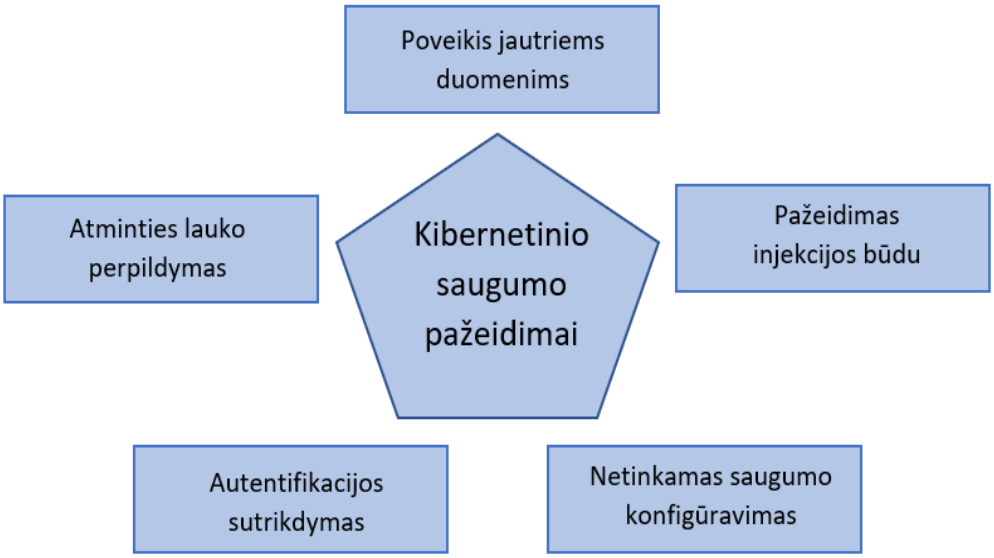
Apibendrinant galima teigti, kad siekiant jog valstybės kibernetinis saugumas būtų sklandžiai užtikrinamas yra būtina jog visos instancijos veiktų bendradarbiavimo principu. Taip pat svarbu jog kibernetinio saugumo politikos kūrėjai, įgyvendintojai ir subjektai periodiškai atliktų kibernetinio saugumo rizikos vertinimus bei pratybas.

3.2. Kibernetinio saugumo pažeidimai: kibernetinių atakų vektoriai

Šiandieninėje visuomenėje tenka išgirsti terminą esą XXI amžių kartais galima vadinti "duomenų amžiumi". Didelė dalis mūsų gyvenimo tikrai prasideda ir baigiasi informacinių sistemų tinklais, kuriuose talpinami įvairūs duomenys. Atsižvelgiant į tai, kad daugelis naudojasi informacinėmis ir ryšių technologijomis (IRT), informacijos, kuri talpinama internete, duomenų saugumas vienu iš svarbiausių aspektų turi būti ne tik duomenų saugotojams, bet ir patiems vartotojams (Padallan, 2019). Kibernetinis saugumas šiuo metu vaidina dar didesnį vaidmenį. Lietuvos Respublikos Kibernetinio saugumo įstatyme kibernetinio saugumo sąvoka suprantama kaip: "visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti" (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

Už kibernetinio saugumo įgyvendinimą viešajame sektoriuje atsakingų žmonių pareiga yra besikeičiant aplinkybėms pritaikyti saugumo priemones taip, kad būtų patenkinti visuomenės poreikiai ir teisė į saugumą.

Šiuo tikslu Padallan (2019) pateikia penkis dažniausiai nutinkančius kibernetinio saugumo pažeidimus visame pasaulyje, šie pažeidžiamumai aktualūs ir elektroninės valdžios portalams (žr. 6 pav.):



6 pav. Kibernetinio saugumo pažeidimai
Šaltinis: Padallan (2019).

Poveikis jautriems duomenims- neigiamas poveikis jautriems duomenims atsiranda tada, kada programa, įmonė ar kitas subjektas netyčia juos atskleidžia. Tam įtaką gali turėti daugybė dalykų, pavyzdžiui, silpnas slaptažodis, slaptažodis be šifravimo, programinės įrangos saugumo trūkumai, klaidingai įkelti duomenis arba asmens duomenys įkelti į nesaugią duomenų bazę. Tai vienas dažniausiai pasitaikančių kibernetinio saugumo pažeidžiamumų (Padallan, 2019). Asmeninius duomenis kenkėjiškiems tikslams galima gauti kol jie nėra sunaikinti ir yra be priežiūros, guli nesaugioje duomenų bazėje arba kol yra perkėlinėjami į kitą sistemą ar duomenų bazę (Padallan, 2019). Programišiai dažnai naudoja kenkėjišką programą pavadinimu angliškų pavadinimu *Man-in-the-middle* (MITM). Ataka vykdoma slapto pasiklausymo forma kuomet užpuolikas įtikina aukas (gavėją ir siuntėją), kad jie tiesiogiai bendrauja vienas su kitu, o iš tikro tai pokalbis yra įsilaužėlio rankose.

2021 metais vasarį vyko Seimo Užsienio reikalų komiteto (URK) vadovo Žygimanto Pavilionio pokalbis su Rusijos provokatoriais, kurie apsimetę Rusijos opozicionieriaus Aleksėjaus Navalno štabo vadovu Leonidu Volkovu kalbėjosi su URK vadovu. Pokalbio metu Pavilionis manęs, kad kalba su opozicionieriumi, sumenkino LR Prezidento vardą ir paties Pavilionio monologas paviešintas kaip neetiškas. Mano nuomone, tai puikus pavyzdys, kaip žmogus, ne būdamas tikras su kuo šneka gali savo kalbas pakreipti ne tik prieš save, bet ir prieš visą valstybę. Pasak paties Pavilionio, ši ataka buvo įvykdyta tam, kad supriešintų ir suskaldytų vakarų valstybes bei buvo įvykdyta prieš trijų Baltijos šalių, taip pat Ukrainos, Jungtinės Karalystės, Kanados ir kitų valstybių politikus. Vilniaus politikos analizės instituto analitiko Laurinavičiaus teigimu, ši ataka yra Rusijos specialiųjų tarnybų provokacija

(Jačauskas, 2021). Mano manymu, ši Rusijos provokacija akivaizdus atakos Man-in-the-middle pavyzdys.

Įterpimo atakos arba **SQL injekcijos (angl. *Structured Query Language Injection*)-** viena iš dažnai pasitaikančių kibernetinių atakų būdų kuomet atakuojamos interneto svetainės, kurios turi duomenų bazes. SQL injekcijos pažeidimai dažniausiai atsiranda, kai žiniatinklio programų kūrėjas ne užtikrina, kad iš žiniatinklio, naudojamų slapukų ar įvesties parametro ir t.t. gautos vertės būtų patvirtintos arba užkoduotos prieš jas perduodant SQL užklausoms, kurios bus vykdomos duomenų bazės serveryje (Hartley, 2012). Svetainės prisijungimo mechanizmas turi patikrinti vartotojo prisijungimo duomenis. Įterpdamas naudingąją apkrovą (angl. *Payload*) į pažeidžiamą prisijungimo puslapį, užpuolikas gali apgauti svetainę suklaidinant, kad buvo pateiktas teisingas vartotojo vardas ir slaptažodis, kai iš tikrųjų užpuolikas žino tik aukos vartotojo vardą (Shema, 2010). Injekcijų trūkumai atsiranda, kai nepatikrinti ir netinkami vartotojo duomenys siunčiami į žiniatinklio programą kaip užklausos dalis. Įsilaužėlio kenkėjiški duomenys apgauna programą, kuomet prašoma vykdyti nenumatytas, neįprastas komandas arba atskleisti asmeninius duomenis. Injekcija įvyksta, kai įsilaužėlis gauna kenksmingą asmeninę informaciją, kuri buvo įvesta į žiniatinklio programą, kuri tada veikė nesaugiai. Tai yra viena seniausių atakų prieš žiniatinklio programas, tačiau ji vis dar yra dažnai naudojama, plačiai paplitusi, tačiau jos galimybės neigiamai paveikti fizinius ir juridinius asmenis vis dar yra labai didelės (Hartley, 2012; Padallan, 2019).

Sukčiavimas apsimetant (angl. *Phishing*)- dar vadinama slaptažodžių žvejojimu (angl. *Password Fishing*), tai tokia sukčiavimo forma prieš organizacijas ar privačius asmenis. Phishing‘o ataka vykdoma pasinaudojant elektroninio pašto dėžutėmis, kuomet siunčiamos suklastotos žinutės ar suklastotais internetiniais tinklalapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius ar kitus konfidencialius duomenis (LR RRT, 2020). Sukčiavimo apsimetant ataka dažniausiai vyksta trimis etapais: nusikaltėlis suranda informacijos apie taikinį- „masalo etapas“, tada naudoja tą taikinį ryšiui sukurti- „kabliuko etapas“ ir, galiausiai naudoja ryšį, kad taikinys atliktų reikiamą veiksmą- „gaudymo etapas“.

„Masalo etapas“- pirmasis sukčiavimo atakos žingsnis yra informacijos pasiruošimas ir rinkimas (Woods, 2021). Siekiama išsiaiškinti kuo daugiau informacijos apie „auką“- darbinė veiklą, laisvalaikio pomėgiai, draugai ir pan. Nusikaltėliai gali surinkti labai išsamią ataskaitą iš vartotojų socialinių tinklų profilių, kad sukurtų labai pritaikytą sukčiavimo pranešimą ir jis neatrodytų kaip kenkėjiškas. Tai yra viena iš priežasčių, kodėl duomenų nutekėjimo pažeidimai gali būti tokie pavojingi: pavyzdžiui, jei

nutekinamas bendrovės ar įstaigos serveriuose esantys el. pašto adresų sąrašas, nusikaltėliai gali siuntinėti el. laiškus apsimesdami, kad rašo iš tos bendrovės ar įstaigos..

„Kabliuko etapas“- antrasis etapas, kai kibernetinis nusikaltėlis jau yra gavęs reikalingą informaciją, bet tam, kad nusikaltėlis įvykdytų ataką jis turi auką išgąsdinti arba kažką pažadėti (Woods, 2021). Dažniausiai sukčiavimo metu tikslas yra priversti auką patikėti, kad jos paskyros privatumas jau buvo pažeistas ir metas priversti auką veikti negalvojant. Tokiu būdu kibernetiniai nusikaltėliai gali nesunkiai suklaidinti vartotojus apsimetant, kad laiškas rašomas iš elektroninių valdžios vartų portalo ir prašoma suvesti asmeninius duomenis, prisijungti. Vartotojus dažnai suklaidinama parašant žodžius: “skubu”; “skola”; “laimėjimas”; “didelė nuolaida” ir pan. Žmonės susijaudina gavę panašaus pobūdžio laiškus ir gali prarasti budrumą, ko ir siekia nusikaltėliai.

„Gaudymo etapas“- Trečioji sukčiavimo fazė yra tikroji ataka. Kibernetinis nusikaltėlis išsiunčia apsimestinį elektroninį laišką ir ruošiasi užbaigti ataką. Šiame etape užpuoliko veiksmai gali būti skirtingi, priklauso kokio rezultato jis siekia. Pavyzdžiui, jei jie naudojo nukreipimo puslapį, kad gautų aukos el. pašto slaptažodį, tada tikslas yra prisijungti prie aukos el. pašto paskyros, kad pasiektų daugiau kontaktų ir galėtų toliau vykdyti atakas (Woods, 2021). Anglijoje ir Velse nuo 2021 metų spalio iki 2022 metų kovo buvo renkami duomenys kuo dažniausiai apsimesdavo kibernetiniai nusikaltėliai: 54 % gavo laiškus nuo apsimetėlių pristatymo kompanijomis; 32 % nuo apsimetėlių bankais ir finansų bendrovėmis; 29 % nuo apsimetėlių ekomercijos įmonėmis; o 25 % nuo apsimetėlių valstybinėmis įstaigomis (Nacionalinės statistikos biuras, 2022).

Dažniausiai sukčiavimo apsimetant atakos būna nukreiptos prieš bankų klientus, siekiant sužinoti jų prisijungimo prie elektroninės bankininkystės sistemų slaptažodžius ar kreditinių kortelių duomenis. Vėliau tokiu būdu gauta informacija gali būti panaudota vykdant nusikalstamas veikas: neteisėtus prisijungimus prie informacinių sistemų, pinigų vagystes iš sąskaitų ar elektroninėje erdvėje atsiskaitant už prekes svetimomis kortelėmis.

XSS (angl. *Cross- site Scripting*) atakos- šis pažeidimo būdas leidžia įsilaužėliui įterpti naršyklėje vykdomą kodą į kitų vartotojų peržiūrimą internetinį puslapį ir taip įsibrauti į aukos asmeninę erdvę ir (Chaudharya ir kt., 2021). XSS dažniausiai remiasi tos pačios kilmės politikos koncepcija, kuri iš esmės leidžia tik to paties puslapio resursams sąveikauti tarpusavyje be jokių specialių apribojimų (Kompiuterinių incidentų tyrimo tarnyba, 2015). XSS atakos metu savavališkai įterptas kodas yra vykdomas aukos naršyklėje, šis kodas paprastai naudojasi papildomomis privilegijomis (pagal tos pačios kilmės politiką). Dažniausiai XSS atakos panaudojamos tokiems tikslams, kaip vartotojo sesijų užgrobimas (*session hijacking*), Web puslapių sudarkymas, kenkėjiško turinio įterpimas, vartotojų nukreipimas į kitus puslapius/turinį ir panašiai (Kompiuterinių incidentų tyrimo tarnyba, 2015).

Netinkamas saugumo konfigūravimas (angl. *Security Misconfiguration*)- šio galimo kibernetinio saugumo pažeidimo esmė yra spragų ir silpnybių ieškojimas. Pavyzdžiui, per lengvų, kodais neužkoduotų ar su inicialais susijusių slaptažodžių naudojimas, numatytųjų slaptažodžių ne pakeitimas, taip pat per retai arba kaip tik per dažnai keičiamų slaptažodžių, kurie tampa nepatikimi, išlaikymas (Padallan, 2019). Jeigu įvykdoma šio tipo ataka, Padallan (2019), o taip pat ir mano nuomone, įsilaužėliai dažnai lengvai pasiekia kliento duomenis, nes patys klientai ne visada yra suinteresuoti juos apsaugoti. Padallan (2019) teigimu, skaitmeninis saugumas yra labai reikšmingas ir turi būti nuolat atnaujinamas. Taip pat, mano nuomone, visuomenėje trūksta kibernetinio švietimo, kuris edukuotų piliečius kaip jie gali padėti sau ir išvengti kibernetinių atakų, kurios paviešintų jų duomenis. Taip pat noriu paminėti, kad šio tipo atakos neretai įvykdomos ir Lietuvoje.

Sesijos sutrikdymo valdymas ir autentifikacija (angl. *Broken Session Management and Authentication)-* autentifikacijos (nustatymo ar atitinka originalą) sesijos turi unikalius identifikatorius, kurie priskiriami konkrečiam vartotojui (Pauli, 2013). Taikymo funkcijos, susijusios su autentifikavimu ir sesijų valdymu, dažnai nėra tinkamai įgyvendinamos, todėl užpuolikai gali sugadinti atpažinimo raktus, slaptažodžius ar pasinaudoti kitomis spragomis norėdami perimti vartotojų tapatybes (Pauli, 2013). Žiniatinklio programa naudodama sesijų valdymą gali sekti kiekvieno vartotojo užklausas. Jeigu nebūtų sesijų valdymo, turėtumėte iš naujo prisijungti po kiekvieno pateikto prašymo. Kaip pavyzdį galima pateikti tiesiog paslaugos užsakymą elektroninių valdžios vartų portale: įsivaizduokite, kad turite prisijungti, kai ieškote reikiamos paslaugos, tada vėl reikalaujama prisijungimo, kai pasirenkate paslaugą, tada vėl, kai ją užsisakote ir vėl, kai norite pateikti savo mokėjimo informaciją. Taigi sesijų valdymas buvo sukurtas, kad vartotojams būtų patogiau ir tereikėtų prisijungti tik pirmo apsilankymo metu, o žiniatinklio programa prisimintų, kuris vartotojas kokią paslaugą vartojas užsisakė (Pauli, 2013). Sesijų valdymas ir autentifikavimas pradžioje nebuvo planuotas, nes jo poreikis atsirado tik atsirado tik išpopuliarėjus internetinei prekybai ir administracinėms paslaugoms teikiamoms internetu. Todėl internetinių svetainių nesugebėjimas tinkamai užkoduoti šifravimo procedūrų leidžia įsilaužėliams pasinaudoti klientų asmeniniais duomenimis ir juos nutekinti (Padallan, 2019).

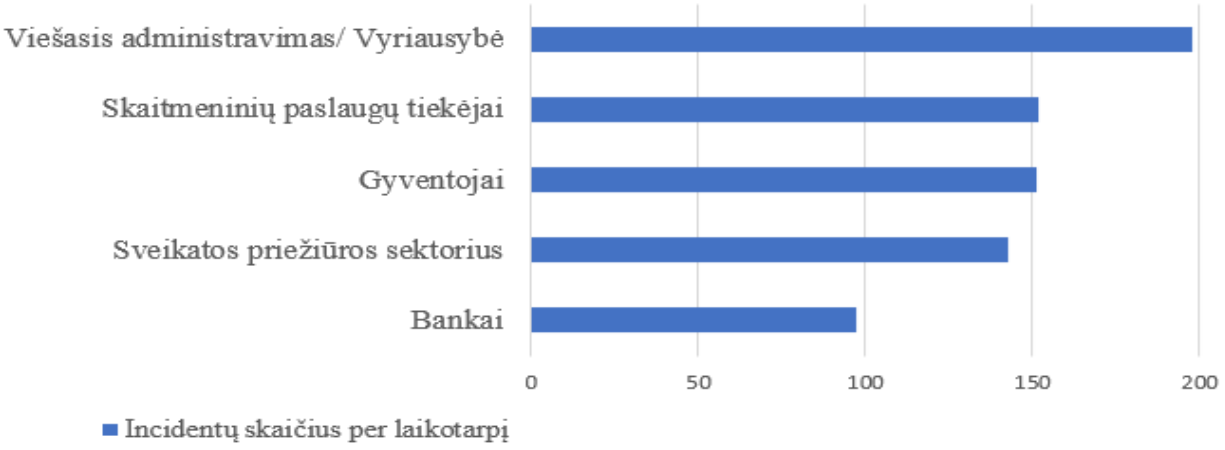
Atminties lauko perpildymas (angl. *Buffer Overflow*)- atakoje, kurios metu vyksta atminties lauko perpildymas, programa saugo didesnį kiekį informacijos negu tai leidžia buferio galimybės. Tokios atakos metu paveikiami ir naudojami kiti panašūs adresai. Valdiklis perrašo informaciją kitiems buferio adresams taip padarydamas žalą arba visai ištrindamas seną informaciją (Padallan, 2019). Galimą aminties lauko (buferio) perpildymo problemą sunku nustatyti, tačiau ją įgyvendinti yra dar

sunkiau, nes įsilaužėlis turi žinoti duomenų bazių atminties lauko pajėgumus. Tačiau, jei įsilaužėlis turi informacijos ir technines galimybes tai padaryti, jis be didelių pastangų gali įvykdyti kibernetinę ataką, siųsdamas programai žymiai didesnį informacijos kiekį, nei ji gali apdoroti ir laikyti savo atminties lauke. Tai padaręs nusikaltėlis gali pasinaudoti naudotojų asmenine informacija kai programa grąžina jų kodus atgal (Padallan, 2019).

Taigi, trumpai apibendrinant galime teigti, kad norint kokybiškai užtikrinti kibernetinį saugumą, reikia gerai žinoti kibernetinių atakų vektorius. Vienas iš didžiausią grėsmę keliančių vektorių dabar įvardijamas kaip sukčiavimas apsimetant (angl. *Password Phishing*). Poskyryjje 3.3.2. pateikiami pasiūlymai ir rekomendacijos kaip apsisaugoti nuo kibernetinių atakų vektorių.

3.2.1. Labiausiai pažeidžiami sektoriai

Nesuvaldytos kibernetinio saugumo grėsmės Europos Sąjungoje daro didelę įtaką visuomenei bei ypatingos svarbos organizacijoms. Europos Sąjungos kibernetinio saugumo agentūra (ENISA) pastebėjo, kad nuo 2020 m. balandžio mėnesio iki 2021 m. liepos mėnesio labiausiai nukentėjo šie penki sektoriai (žr. 7 pav.):



7 pav. Labiausiai kibernetinių incidentų pažeidžiami sektoriai
Šaltinis: Europos Sąjungos agentūra (2021)

Minėtu laikotarpiu užfiksuoti 198 incidentai viešajame sektoriuje ir vyriausybėse, skaitmeninių paslaugų teikėjų erdvėje 152 incidentai, gyventojus sutrikdė 151 incidentai, sveikatos priežiūros sektorių 143 incidentai ir bankus 97 incidentai. Duomenys rodo, kad jautriausiu išlieka vyriausybinis sektorius, todėl jo kibernetinio saugumo užtikrinimas turėtų būti prioritetinis.

Pandemijos laikotarpis buvo kupinas permainų, įmonės ir įstaigos turėjo greitai prisitaikyti prie kintančių aplinkybių bei darbo perkėlimo į nuotolį. Nors daugumai darbuotojų tai patogus būdas atlikti savo darbus, tačiau kibernetinį saugumą užtikrinantiems darbuotojams tai tikras iššūkis, nes būtent saugumo spragos yra galimybės kibernetiniams nusikaltėliams. Europos Sąjungos kibernetinio saugumo agentūra konkrečiai išskyrė 9 pagrindines kibernetines grėsmes:

- **Išpirkos prašymas (angl. *Ransomware*)** – užpuolikai užšifruoja organizacijos duomenis ir reikalauja sumokėti išpirką, kad būtų atkurta prieiga. Ransomware šiuo metu laikoma pavojingiausia grėsme. Tai kenkėjiška programinė įranga, skirta neleisti vartotojui ar organizacijai pasiekti savo kompiuteryje esančių failų. Užpuolikai reikalauja sumokėti išpirką, kad atkurtų prieigą. Pateikti duomenys rodo, kad vidutinė išpirkos suma padvigubėjo nuo 71 000 eurų 2019 metais iki 150 000 eurų 2020 metais. Apskaičiuota, kad 2021 metais. pasaulinė išpirkos programa pasiekė 18 milijardų eurų žalą – t. y. net 57 kartus daugiau nei 2015 metais. Laikotarpis per kurį organizacija būdavo visiškai suparalyžiuota 2021 metais buvo vidutiniškai 23 dienos, o išpirkos reikalaujančios ataka įvykdao maždaug kas 11 sekundžių (Europos Parlamentas, 2022).
- **Kriptovaliutos kasimas (angl. *Cryptojacking*)** – kai kibernetiniai nusikaltėliai slapta naudoja aukos kompiuterinę galią kriptovaliutai generuoti.
- **Grėsmė duomenims (angl. *Threats against data*)** – duomenų pažeidimai/nutekėjimai
- **Kenkėjiška programa (angl. *Malware*)**– programinė įranga, suaktyvinanti procesą, kuris kenkėjiškai veikia sistemą.
- **Dezinformacijos skleidimas (angl. *Disinformation*)**– klaidinančios informacijos skleidimas.
- **Nepiktybinės grėsmės (angl. *Non-malicious threats)*** – žmogiškosios klaidos ir neteisingos sistemos konfigūracijos.
- **Grėsmės prieinamumui ir vientisumui (angl. *Threats against availability and integrity)*** – atakos, neleidžiančios sistemos vartotojams pasiekti savo informacijos taip blokuojančios prieinamumą ir vientisumą.
- **Su el. paštu susijusios grėsmės (angl. *Email-related threats)*** – tokiu būdu užpuolikai siekia manipuliuoti žmonėmis, kad jie taptų el. pašto atakos aukomis;
- **Tiekimo grandinės grėsmės (angl. *Supply chain threats)*** – užpuolimas, pavyzdžiui, paslaugų teikėjas, siekiant gauti prieigą prie kliento duomenų (Europos Komisija, 2021).

Taigi, remiantis 7 paveikslu matome, kad vienas dažniausiai kibernetinių užpuolikų pažeidžiamų sektorių yra valstybinis viešasis sektorius. Siekiant kuo labiau susitiprinti būtent šio sektoriaus kibernetinę saugą reikia žinoti ne tik pagrindines grėsmes, bet ir būdus kaip tų grėsmių išvengti.

Skyrelyje 3.3.2. Kibernetinio saugumo stiprinimo būdai plačiau aprašomi veiksniai kaip galima sušvelninti kibernetinius pažeidimus ir išvengti kibernetinių atakų.

3.3. Valstybinių įstaigų kibernetinio saugumo pažeidimai Lietuvoje

Šiuolaikiniame pasaulyje, kuomet informacinės sistemos nuolat tobulėja, daugelis sričių persikelia į elektroninę erdvę, elektroninėje erdvėje vykdomų įvairių nusikalstamų veikų skaičius Lietuvoje bei visame pasaulyje nuolat didėja ir prognozuojama, kad ir toliau didės. Tobulėja ne tik kibernetinis saugumas, elektroninės apsaugos sistemos, bet ir nusikaltėliai, kurių tikslas pasipelnyti vykdant kibernetines atakas ir kitus nusikaltimus elektroninėje erdvėje (LR Prokuratūra, 2019). LR baudžiamojo kodekso skyriuje elektroninių duomenų ir informacinių sistemų saugumas nurodomas kaip vienas iš pagrindinių objektų nusikalstamai veikai vykdyti. Neteisėtas disponavimas elektroniniais duomenimis apima tokius kibernetinius nusikaltimus kaip tinklalapio „nulaužimas“; neteisėtas prisijungimas prie tinklalapio turinio ir jo valdymo; sistemos ir elektroninių duomenų pakeitimas ar pašalinimas; neteisėtas poveikis informacinei sistemai (pvz.: DoS ir DDoS atakos prieš internetinius puslapius, tarnybines stotis (LR Prokuratūra, 2019). DoS ir DdoS atakos, tai turbūt dažniausiai pasitaikančios atakos, kurių pagrindinis tikslas paveikti IS arba visą tinklą, kad vartotojai negalėtų pasiekti reikiamo puslapio, nes puslapio serveriai neatlaikytų tokios didelės tinklo apkrovos, o jų asmens duomenis būtų galima neteisėtai periimti ir pasinaudoti. Tokio tipo atakos gali ištikti įvairaus pobūdžio interneto svetaines, tačiau, jeigu kibernetinių atakų taikiniu tampa ypatingos svarbos viešųjų ir administracinių paslaugų sistemos, pavyzdžiui, SoDra, VMI, Elektroniniai valdžios vartai, tai pavojus gali kilti ne tik pavieniams vartotojams, bet ir visos valstybės asmeniniams duomenims (Prokuratūra, 2019). Šiuolaikiniai kibernetiniai nusikaltimai išsiskiria dar ir tuo, kad jie dažniausiai vykdomi ne pavienių asmenų, o buriamos gaujos, organizuotos grupės, kurios veikia skirtingose pasaulio šalyse, todėl jų identifikavimas ir nusikalstamų veikų ištyrimas yra itin sunkus ir sudėtingas procesas (LR Prokuratūra, 2019).

Todėl, apibendrinant galima daryti išvadą, kad aktyvus dėmesys stipriam kibernetinio saugumo užtikrinimui ypatingai svarbus valstybinio sektoriaus internetiniams puslapiams, nes jų serveriuose yra patalpinti kone visos šalies gyventojų jautrūs asmeniniai duomenys, o juos būtina apsaugoti. Ypatinga svarbu, kad kibernetinės atakos negalėtų paveikti valstybinės reikšmės serverių ir programų, kad nebūtų sutrikdytas sklandus elektroninis valstybės valdymas.

3.3.1. Kibernetiniai incidentai elektroniniuose valdžios vartuose

Internetinių svetainių pažeidžiamumas atsirado kartu su didėjančiu susidomėjimu ir dažnesniu interneto naudojimu. Pagal Nacionalinio kibernetinio saugumo centro parengtą 2021 metų pirmo ketvirčio ataskaitą, per šį laikotarpį lyginant su 2019 metų I ketvirčiu kibernetinių incidentų skaičius išaugo 33,3%, t.y. net 1045 incidentai. Tarp jų užfiksuoti 43 vidutinės/ didelės reikšmės incidentai. Tai reiškia, kad ne visi kibernetiniai pažeidimai yra toleruotini. Jeigu pasikėsinama į ypatinguosius duomenis, kurių atskleidimas gali turėti žalingą poveikį asmeniui, organizacijai ar visuomenei bei valstybei, gali kilti didelio masto šiuolaikinė tragedija. Elektroninių paslaugų vartotojams gerai žinoma, kad norint prisijungti prie elektroninių valdžios vartų būtina pateikti savo asmens duomenis ir prisijungti per banką arba naudojantis mobiliuoju parašu. Toks prisijungimo sugriežtinimas įvestas ne veltui. Bendrovės, teikiančios informacinio saugumo užtikrinimo paslaugas direktorius Lučinskis 2010 metais liepos mėnesį pastebėjo ir perspėjo, kad norint prisijungti prie Elektroninių valdžios vartų portalo tereikia tik žinoti asmens kodą, o žinant asmens kodą galima prisijungti ne tik prie savo, bet ir prie bet kurio žmogaus paskyros. Žinoma, toks neteisėtas kito asmens duomenų naudojimas laikomas nusikalstama veika ir už tai gresia baudžiamoji atsakomybė (LR BK 198 str., 2007).

Todėl tokio saugumo e. valdžios vartų portalui neužteko (Jackevičius, 2010). Trakimavičius paantrino, kad norint pasinaudoti tokia portalo spraga būtina aukšta kompetencija sistemų saugos srityje. Taigi, specialisto teigimu, paprastam interneto naudotojui tokia spraga pasinaudoti esą nebūtų įmanoma (BNS, 2010). Tačiau objektyviai vertinant praeities situaciją, nesvarbu, kad portalo kibernetinio saugumo spraga galbūt iš pažiūros įveikiama tik rimtam specialistui, toks sistemos pažeidžiamumas galėjo būti puikus šansas įsilaužėliams (angl. *Hackers*) pasipelnyti ir neteisėtai disponuoti naudotojų asmens duomenimis.

Apie saugumą viešojo sektoriaus interneto svetainėse rašė ir Nacionalinis kibernetinio saugumo centras (toliau- NKSC) savo 2017 metų ataskaitoje. NKSC atliko du internetinių svetainių saugos patikrinimus. Pagal sąrašą buvo patikrinta 1200 viešajam sektoriui priskiriamų svetainių adresų. Tyrimas buvo atliktas remiantis statistiniu modeliavimu, analizuojant įprasto svetainės naršymo metu gautą informaciją, techninius duomenis, gautus iš duomenų bazių, ir pasyvaus skenavimo priemonėmis gautą informaciją apie prieglobos tarnybinių stočių ir svetainės transliavimo tarnybų programinę įrangą. Atlikus tyrimą, nustatyta, kad 23 proc. tirtų viešojo sektoriaus svetainių gali būti sutrikdytos žemos kvalifikacijos, 52 proc. vidutinės ir 25 proc. aukštos kvalifikacijos įsibrovėlių (NKSC, 2017). Taigi anksčiau minėto specialisto įžvalga, kad norint pasinaudoti kibernetinio saugumo spragomis reikia aukštos kompetencijos, mano nuomone, nėra teisinga. Po 7 metų tyrimas akivaizdžiai parodė, kad norint sutrukdyti viešojo sektoriaus interneto portalus daugumai įsibrovėlių pakaktų vidutinės kvalifikacijos. Lyginant 2016 metų skaičiavimus pastebėta, kad tuomet į 18 procentų viešojo sektoriaus internetinių

svetainių buvo galima įsilaužti neturint techninių žinių ar ypatingų programavimo įgūdžių, į 34 proc. svetainių buvo galima įsilaužti, turint įgūdžių ir žinių, o 48 proc. svetainių buvo sąlygiškai saugios, į jas įsilaužti reikėtų kvalifikuotų specialistų žinių (NKSC, 2017). Šioje vietoje peršasi išvada, kad kuomet mažesnis skaičius internete teikiamų viešųjų ir administracinių paslaugų, tuo paprasčiau jas apsaugoti. IVPK statistikos duomenimis, 2016 metais 45 procentai gyventojų naudojosi internetu prieinamomis viešosiomis ir administracinėmis paslaugomis, o 2017 metais skaičius paaugo 2%, iki 47 procentų (IVPK, 2021).

Dar viena Elektroninių valdžios vartų saugumo grėsmė pastebėta 2019 metais. Šią spragą pastebėjo vadinamasis "baltakepuris". Taip lietuviškai vadinami etiški įsilaužėliai (angl. *White Hats*), kurie dažniausiai būna kibernetinio saugumo ekspertai savo metodikomis bandantys ir tikrinantys informacinių sistemų saugumą (Lrt.lt). Dėl teisinio kibernetinių spragų reglamentavimo trūkumo, rastos spragos dažnai lieka neatskleistos, o juos suradę kibernetinio saugumo tyrinėtojai, ekspertai, "baltakepuriai" rizikuoja užsitraukti administracinę arba baudžiamąją atsakomybę (Maji ir kt.,2022).

Taigi, jeigu viešųjų ir administracinių paslaugų portalai nėra pilnai apsaugoti, dar daugiau internetinių paslaugų vartotojų gali nukentėti nuo įsilaužėlių. Rašant magistrinį darbą ir beieškant informacijos interneto šaltiniuose bei moksliniuose straipsniuose, pastebėta, kad susirūpinimas elektroninių valdžios vartų portalo kibernetiniu saugumu nors ir nėra naujiena, tačiau ir toliau labai aktuali tema. Renkant informaciją taip pat analizuoti būdai kuriais būtų galima išvengti arba sušvelninti kibernetines atakas vykstančias viešųjų paslaugų tiekimo portaluose.

3.3.2. Kibernetinio saugumo stiprinimo būdai

Kibernetinių atakų vektorių skyriuje aprašytos grėsmės nėra tik literatūrinės, jos kelia realų pavojų tiek paprastoms interneto svetainėms, tiek elektroninių valdžios vartų portalui. Spėjama, kad kibernetinių atakų visiškai neišvengsime, nes jos nuolat tobulėja ir kinta, tačiau jų poveikį ir žalą žinant apsisaugojimo galimybes galima kontroliuoti ir švelninti. Kibernetinis saugumas nėra vien bendrovių, kurių duomenų bazėse yra patalpinti mūsų asmens duomenys, reikalas. Mano nuomone, svarbu ugdyti visos visuomenės supratimą kas yra tas kibernetinis saugumas, kodėl jį būtina užtikrinti ir kodėl visuomenė šiame procese turi dalyvauti aktyviai. Remiantis naujausia moksline literatūra bei medžiaga internete, pateikiami pasiūlymai kuriais vadovaujantis siekiama užtikrinti elektroninių valdžios vartų saugumą.

Informacijos šifravimas ir atsarginių kopijų kūrimas

Dažniausiai nusikaltėlių žinios apie kibernetinį saugumą būna didesnės nei asmenų, kurių saugumą bandoma pažeisti žinios. Todėl norint apsaugoti jautrius duomenis juos būtina šifruoti. Šifravimas užtikrina duomenų saugumą, kad net jeigu jie pateks į įsilaužėlių akiratį, jais nebus galima pasinaudoti. Kai kuri duomenų šifravimo programinė įranga netgi leidžia žinoti, kai kiti žmonės bando pakeisti arba sugadinti informaciją (Sukianto, 2022). Taip pat efektyvus kibernetinio saugumo užtikrinimo būdas- atsarginių kopijų kūrimas, nes kartais augumo pažeidimai gali sukelti duomenų praradimą, o neturint patikimos ir saugios atsarginės duomenų kopijos, tai gali sukelti veiklos sutrikimų, dėl kurių organizacija gali prarasti daug pajamų gali patirti didelių nuostolių (Sukianto, 2022). Sukianto (2022) įvardija efektyvią atsarginių kopijų kūrimo strategiją „3-2-1 taisyklę“. Remiantis šia strategija, pravartu turėti bent tris saugomų duomenų kopijas: dvi iš jų turėtų būti saugomi skirtingose laikmenose, o vienas turėtų būti laikomas su įstaiga nesusijusioje vietoje.

Reguliarūs darbuotojų mokymai

Vienas iš dažniausiai pasitaikančių kibernetinių atakų būdų yra kuomet įsilaužėliai gauna prieigą prie duomenų bazės per darbuotojams siunčiamus elektroninius sukčiavimo laiškus. Statistika rodo, kad visame pasaulyje išsiunčiama daugiau nei 3,4 milijardų kenkėjiškų laiškų su nuorodomis, kurios suteikia įsilaužėliams prieigą prie naudotojo duomenų, įskaitant prisijungimo duomenis (Sukianto, 2022). Įsilaužėliai stengiasi, kad siunčiami sukčiavimo laiškai atrodytų kaip tikri ir teisėti. Pavyzdžiui, įsilaužėlis gali išsiųsti el. laišką, kuriame apsimetinėja organizacijos ar įstaigos vadovais, prašydamas asmeninės informacijos, prisijungimo duomenų (Sukianto, 2022). Darbuotojas, kuris nė karto nedalyvavo kibernetinio saugumo mokymuose arba jo darbovietėje tokiems mokymams neteikiamas prioritetas ir pirmenybė, vargu ar gali turėti reikiamų žinių kaip tokius laiškus atpažinti. Todėl nenuostabu, kad be tinkamo mokymo darbuotojas gali atskleisti slaptą informaciją (Sukianto, 2022). Todėl labai svarbu jog valstybinės įstaigos ir organizacijos reguliariai vykdytų kibernetinio saugumo mokymus ir pratybas darbuotojams, nes nuo to priklauso ne tik organizacijos, tačiau ir daugelio piliečių duomenų saugumas.

Kelių lygių autentifikavimas

Kaip anksčiau minėta, jungiantis prie elektroninių valdžios vartų reikia jungtis per elektroninę bankininkystę. Lietuvoje daugelis interneto bankų tapatybei patvirtinti ir prisijungti prie interneto banko naudoja kelių lygių apsaugą. Interneto bankų saugumas užtikrinamas trijų lygių apsaugos sistema.

Kiekvienas asmuo sudaręs internetinės bankininkystės paslaugų sutartį gauna priemones, kurios reikalingos jo tapatybei identifikuoti ir mokėjimų operacijoms patvirtinti (LR RRT, 2020).

Naudotojo numeris (ID)– tai identifikavimo kodas, įrašytas internetinės bankininkystės sutartyje. Tai nekeičiamas unikalus ženklų rinkinys, pagal kurį bankas identifikuoja naudotoją (LR RRT).

Naudotojo slaptažodis– tai slaptažodis, kuris pateikiamas užklijuotame voke. Šį slaptažodį reikia pakeisti po pirmos sėkmingos registracijos internetinės bankininkystės tinklalapyje (LR RRT). Šio slaptažodžio pakeitimas į sudėtingą, geriausia 12-16 raidžių ir skaitmenų sudarytą slaptažodį, kurį sudarytų kelių žodžių junginys, kurio prasmė būtų tik jums žinoma.

Kintamas slaptažodis (slaptažodžių kortelė arba generatorius): slaptažodžių kortelė– tai plastikinė daugkartinio naudojimo kortelė ant kurios pateikiami atspausdinti slaptažodžiai- PIN kodai. Kai kurie bankai suteikia papildomą saugumo priemonę- arba ant popieriaus išspausdinti slaptažodžiai, dar vadinami TAN arba PIN2 kodais, kurie suteikiami kiekvienai mokėjimo operacijai. Naudotojas jungdamasis prie elektroninės bankininkystės, turi įvesti atsitiktinai parinktą kodą (LR RRT); slaptažodžių generatorius– tai saugiausia naudotojo tapatybės nustatymo priemonė, užtikrinanti neribotą skirtingų slaptažodžių kiekį. Slaptažodžių generatorius naudojamas prisijungiant prie internetinės bankininkystės sistemos ar (ir) patvirtinant mokėjimo operacijas (LR RRT). Vietoje slaptažodžių kortelės arba generatoriaus bankai jau siūlo naudotis elektroniniu parašu ar mobiliuoju elektroniniu parašu, nes tai laikoma saugesne ir naujoviškesne asmens tapatybės patvirtinimo priemone.

Kelių lygių autentifikavimas taikomas taip pat jungiantis prie socialinių tinklų ar elektroninio pašto svetainės. Pirmo lygio autentifikavimas vyksta slaptažodžio pagalba, o antro lygio autentifikavimas dažniausiai atliekamas įvedant patvirtinimo kodą gautą trumpąja žinute arba Smart - ID pagalba. Tokiu būdu net ir žinant vartotojo slaptažodį paskyrą nulaužti sudėtinga, nes patvirtinimo kodas gaunamas į vartotojo telefoną.

HTTPS protokolas

Ryšio saugumui tarp kliento ir banko tinklalapio užtikrinti paprastai naudojamas HTTPS protokolas paremtas SSL technologija. HTTPS (angl. *Hypertext Transfer Protocol Secure*)– įprasto hipertekstų persiuntimo protokolo (HTTP) plėtinys, palaikantis šifravimą. HTTP protokolas buvo nepakankamai saugus, nes be šifravimo duomenys perduodami tiesiog atviru tekstu. O duomenys perduodami HTTPS pagalba, „supakuojami“ į kriptografinius SSL ar TLS protokolus, taip užtikrinant perduodamų duomenų saugumą (LR RRT, 2020). HTTPS plačiai naudojamas ryšio saugumui užtikrinti interneto svetainėse, ypač ten, kur vyksta elektroninė prekyba ar asmens duomenų mainai. HTTPS padeda apsaugoti duomenis nuo „trečiųjų asmenų“, tai yra ypač svarbu, jeigu vartotojas priverstas naudotis nesaugiais interneto ryšio kanalais- nesaugus wifi, viešasis internetas ir panašiai. HTTPS yra

palaikomas visų modernių naršyklių, tačiau šiuo metu ne visos leidžia pasinaudoti HTTPS teikiamais privalumais (LR RRT, 2020). Žinoma atvejų, kai suklastojami HTTPS protokolai, todėl vienas iš lengviausiai atpažįstamų požymių- HTTPS palaikančių puslapių adresai prasideda *https://* vietoje įprastinio *http://*, kas parodo, jog naudojamas HTTPS ryšys. Paslauga naudojanti HTTPS ryšį turi turėti galiojantį sertifikatą, kuris išduotas patikimo sertifikatų centro (LR RRT, 2020). Kartais svetainių kūrėjai naudoja „self-signed“ arba „savo sugeneruotus“ sertifikatus, kurie nors ir užtikrina, kad kanalas užšifruotas, neįrodo, jog sertifikatas tikrai priklauso organizacijai, todėl kibernetiniai nusikaltėliai gali mėginti „pakišti“ savo sugeneruotus sertifikatus siekdami suklaidinti ar apgauti vartotojus (LR RRT, 2020).

Reguliarus programinės įrangos ir sistemų atnaujinimas

Programinės įrangos ir sistemos naujiniai daro didelę įtaką kibernetinei ir skaitmeninei saugai (Sukianto, 2022). Taip yra todėl, kad reguliarus programiņįs įrangos ir sistemų atnaujinimas leidžia įdiegti naujas funkcijas, ištaisyti klaidas, rasti saugos trūkumus ir juos panaikinti. Įsilaužėliai gali naudoti įsilaužimo kodus, juos pateikti kaip kenkėjišką programos atnaujinimą, kuris gali sutrikdyti sistemos veikimą (Sukianto, 2022). Todėl pravartu įsitikinti, kad svarbiose įstaigų kibernetinėse sistemose naudojama atnaujinimo valdymo sistema, kuri automatiškai nuskanuotų visus atnaujinimo paketus taip užtikrinant, kad nebus instaliuotas kenkėjiškas atnaujinimas.

Apibendrinant galima teigti, kad jei valdžios ir kitų Lietuvai svarbių valstybinių įstaigų portaluose kibernetinis saugumas užtikrinamas minėtais saugos įrankiais, kibernetinių atakų būtų galima beveik visiškai išvengti arba jas įvykdyti įsilaužėliams būtų daug sunkiau. Išanalizuoti kibernetinių atakų vektoriai bei jų prevencijos būdai yra geras pagrindas atlikti kokybinį tyrimą - ekspertų apklausą. Analizės pagrindu atlikta ekspertų apklausa, šios apklausos galimi rezultatai padėtų pagrįsti teiginį, kad visose valstybinės reikšmės portaluose kibernetiniam saugumui veikti ir įgyvendinti, svarbiausia užtikrinti ir kiek įmanoma sumažinti žmogiškosios klaidos galimybę.

4. E. VALDŽIOS SISTEMŲ TOBULINIMO NACIONALINIO KIBERNETINIO SAUGUMO KONTEKSTE TYRIMAS

4. 1. Tyrimo metodologija

Tyrimui buvo pasirinktas **kokybinis tyrimo metodas** - ekspertų nuomonę norima išsiaiškinti standartizuoto interviu arba klausimyno forma. Teigiama, kad tokiu būdu gauti duomenys pateikia išsamesnę informaciją apie nagrinėjamą objektą, nei gauti kiekybiniais tyrimais (Tidikis, 2003, p. 357). Ekspertams asmeniškai buvo pateikta 12 klausimų anketa (žr. 1 priedą), su jais betarpiškai bendraujama su anketa susijusiais klausimais. Pateikta anketa atitinka bendruosius anketos reikalavimus (Kardelis, 2002, p. 93- 94):

- Motyvuotai, logiškai paaiškinta, kokiu tikslu atliekamas tyrimas;
- Respondento pastangos atsakyti turi būti minimalios, todėl sugalvoti konkretūs klausimai su suprantamais atsakymų variantais;
- Dauguma klausimų buvo uždaro tipo, kad anonimiškumas būtų išlaikytas;
- Anketa nesudėtinga ir konkreti, stengtasi pateikti vienas su kitu susijusius klausimus;
- Kad anketa būtų korektiška daugelyje klausimų pateikta daugiau atsakymo variantų, palikta galimybė jei neranda tinkamiausio atsakymo respondentas gali įrašyti savo nuomonę;
- Vengta sudėtingų ir erzinančių klausimų.

Tyrimo problema. Nėra iki galo nustatyta kokios spragos gali lemti jog kibernetinis saugumas valstybinėse įstaigose nėra iki galo užtikrintas. Taip pat nėra žinomi veiksniai, sąlygojantys sklandų kibernetinio saugumo užtikrinimą valstybinėse įstaigose.

Tyrimo objektas. Darbuotojų kibernetinių žinių pritaikymas praktikoje.

Tyrimo tikslas. Išsiaiškinti kaip susijusių sričių ekspertai vertina jų įstaigose atliekamą kibernetinio saugumo užtikrinimą.

Tyrimo uždaviniai:

1. Atlikti ekspertų nuomonės tyrimą, kuris padėtų sužinoti prokuratūros ir kariuomenės ekspertų požiūrį apie kibernetinį saugumą jų įstaigose;
2. Pasiūlyti alternatyvius būdus kaip galima būtų sustiprinti saugumą;
3. Buvo pasirinktas kokybinis tyrimo metodas – ekspertų nuomonės tyrimas struktūrizuoto interviu arba klausimyno forma.

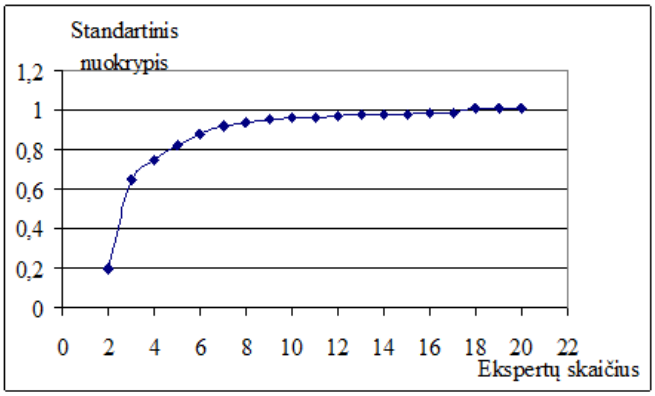
Formuluojant tyrimo klausimus buvo remtasi literatūra. Nurodytas tyrimo tikslas, respondentai supažindinti su keliamos problemos aktualumu. Pažymėta, jog klausimynu siekiama išsiaiškinti jų kaip ekspertų požiūrį į kibernetinio saugumo užtikrinimą valstybinėse įstaigose Lietuvoje, jų atsakymus pateikiant kaip asmeninę nuomonę, vertinimus, o ne organizacijos poziciją. Anketoje nurodyti svarbiausi paaiškinimai ir instrukcija, kaip reikia pildyti tam tikras klausimyno dalis.

Tyrimo organizavimas. Tidikis (2003), teigia, jog vienas efektyviausių tyrimų metodų yra interviu. Iš galimų interviu tipų buvo pasirinktas formalus interviu. Interviu vyko pagal iš anksto suformuluotus klausimus, respondentai į klausimus atsakinėjo ta pačia tvarka. Ši forma pasirinkta siekiant gauti informaciją, ekspertų nuomonę, kurią vėliau būtų galima susisteminti ir išanalizuoti. Formuluojant tyrimo klausimus buvo remtasi literatūra. Nurodytas tyrimo tikslas, respondentai supažindinti su keliamos problemos aktualumu. Pažymėta, jog klausimynu siekiama išsiaiškinti jų kaip ekspertų požiūrį į kibernetinio saugumo užtikrinimą valstybinėse įstaigose Lietuvoje, jų atsakymus pateikiant kaip asmeninę nuomonę, vertinimus, o ne organizacijos poziciją. Anketoje nurodyti svarbiausi paaiškinimai ir instrukcija, kaip reikia pildyti tam tikras klausimyno dalis.

Tyrimas buvo atliekamas 2022 m. lapkričio 8-28 dienomis.

Tyrimas buvo atliekamas apklausiant valstybinių įstaigų darbuotojus- Klaipėdos apygardos prokuratūroje prokurorus ir skyrių vyriausiuosius prokurorus bei Lietuvos Respublikos Ginkluotųjų pajėgų kariniame dalinyje, konkrečiai Lietuvos didžiojo kunigaikščio Butigeidžio dragūnų batalione leitenantus ir vyr. leitenantus. Iš kiekvienos įstaigos buvo apklausta po 9 ekspertus.

Pasirinktas būtent 9 ekspertų skaičius iš vienos institucijos, nes nustatant pakankamą ekspertų skaičių reikia vadovautis metodologinėmis prielaidomis. Teorija teigia, kad sprendimų patikimumą ir priimančių sprendimą (šiuo atveju ekspertų) skaičių sieja ryšys (žr. 8 pav.)



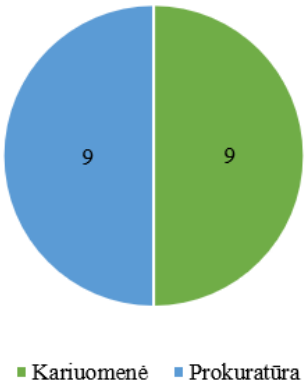
8 pav. Ekspertų skaičiaus pasirinkimas
Šaltinis: Beleţentis ir Žalimaitė (2011)

Matome, kad sprendimų ir vertinimų tikslumas yra pakankamai didelis, kai ekspertų skaičius pasiekia 9. Po to tikslumas kyla labai nežymiai, todėl 9 ekspertų pakanka gauti tiksliai informacijai. Yra įrodyta, kad grupės sprendimų ir įvertinimo tikslumas nenusileidžia didelės ekspertų grupės sprendimų ir vertinimų tikslumui (Baležentis, Žalimaitė, 2011).

4.2. Tyrimo duomenų analizė

Grafikams ir diagramoms kurti panaudota Microsoft Exel programa.

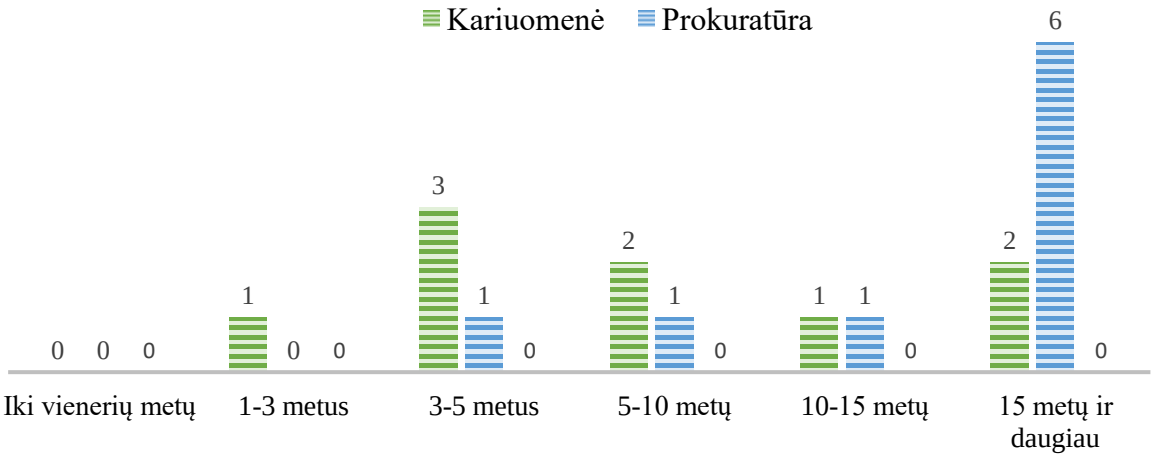
Tam, kad būtų galima efektyviausiai palyginti gautus duomenis buvo apklaustas vienodas skaičius abiejų institucijų darbuotojų. Atliktame tyrime dalyvavo 18 ekspertų (žr.9 pav.):



9 pav. Ekspertų dalyvavimo tyrime skaitinė išraiška

Atliktame tyrime dalyvavo 9 Klaipėdos apygardos prokuratūros prokurorai (4 skyrių vyriausieji prokurorai ir 5 prokurorai) ir 9 Lietuvos didžiojo kunigaikščio Butigeidžio dragūnų bataliono karininkai (4 vyr. leitenantai ir 5 leitenantai).

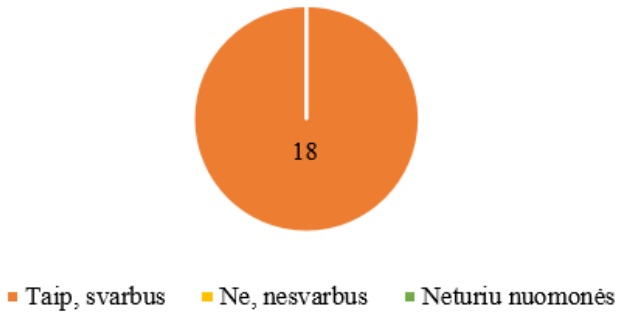
Tolimesnis tyrimo tikslas buvo išsiaiškinti kokia ekspertų darbo patirtis prokuratūroje ir kariuomenėje (žr. 10 pav.):



10 pav. Ekspertų patirtis

Matome, kad daugiausiai prokurorų dirba daugiau nei 15 metų (6 respondentai), po vieną respondentą dirba nuo 3 iki 5; nuo 5 iki 10 ir nuo 10 iki 15 metų. Tuo tarpu tik 2 karininkai kariuomenėje dirba daugiau nei 15 metų, taip pat du karininkai dirba nuo 5 iki 10 metų. Taip pat tik vienas karininkas dirba nuo 10 iki 15 metų bei nuo 1 iki 3 metų. Didžiausias skaičius apklaustųjų kariuomenėje dirba nuo trijų iki penkių metų.

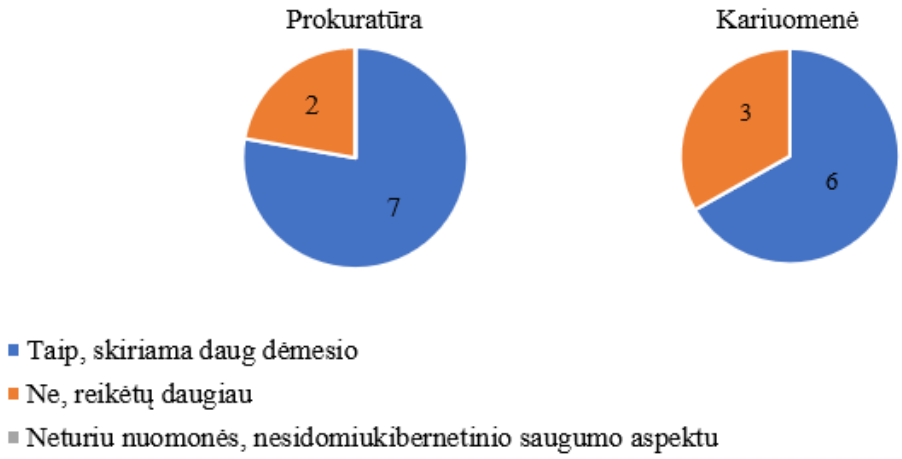
Kitu klausimu buvo siekiama sužinoti respondentų nuomonę apie kibernetinio saugumo svarbumo aspektą jų darbovietėje (žr. 11 pav.):



11 pav. Ekspertų nuomonė dėl kibernetinio saugumo aspekto svarbumo jų darbovietėje

Remiantis skrituline diagrama aiškiai matoma, kad visi 18 respondentų, tiek 9 prokurorai, tiek 9 karininkai, kibernetinio saugumo užtikrinimo svarbumą jų darbovietėje įvardino kaip svarbų. Todėl galime daryti išvadas, kad tiesa, jog ne tik privačiame sektoriuje, bet ir valstybinėse įstaigose didinamas kibernetinio saugumo svarbumas, šią sritį darant prioritetine.

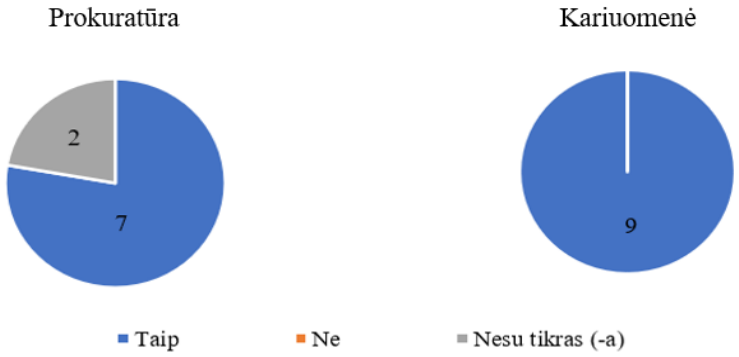
Svarbu išsiaiškinti ar skiriamo dėmesio kibernetinio saugumo klausimams respondentų darbovietėse pakanka. Vizualiai galime matyti kaip pasiskirstė institucijų ekspertų nuomonės (žr. 12 pav.):



12 pav. Ekspertų nuomonė apie dėmesį skiriamą kibernetiniam saugumui jų darbe

Ekspertų balsai abiejose darbovietėse pasiskirstė netolygiai. Septyni iš devynių balsavusiųjų prokurorų atsakė, kad jų nuomone kibernetinio saugumo klausimams jų darbovietėje skiriama pakankamai daug dėmesio. Du prokurorai nurodė, kad skiriamas dėmesys nepakankamas. Tuo tarpu šeši karininkai įvardijo, kad skiriamas didelis dėmesys kariuomenės kibernetinio saugumo klausimams. Trys karininkai atsakė, kad jų nuomone skiriamo dėmesio nepakanka.

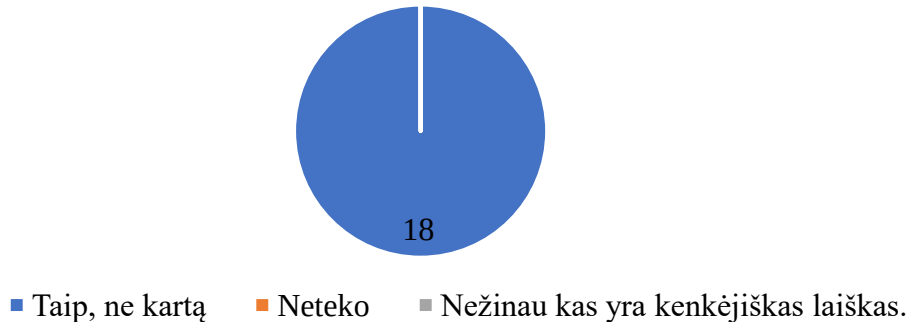
Svarbu sužinoti ar minėtų institucijų darbuotojai žino kur kreiptis pastebėjus vykstantį arba jau įvykusį kibernetinio saugumo pažeidimą (žr. 13 pav.). Vizualiai ekspertų balsai pasiskirstė taip:



13 pav. Ekspertų nuomonė kur kreiptis pastebėjus pažeidimą

Respondentų apklausa rodo, kad 7 prokurorai mano, kad žino kur gali kreiptis pastebėjus kibernetinio saugumo pažeidimą, du respondentai nėra tikri ar jų žinios geros. Tuo tarpu visi 9 karininkai respondentai atsakė jog jiems žinoma kur galima kreiptis pastebėjus kibernetinio saugumo pažeidimą. Galime daryti išvadą, kad karininkai yra geriau informuoti ką reikėtų daryti pastebėjus pažeidimą, prokurorų žinios silpnesnės.

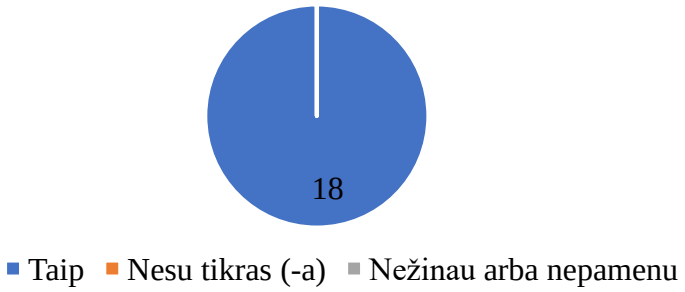
Siekiant susidaryti kuo detalesnį vaizdą apie tai kiek respondentai yra susipažinę su kibernetiniu saugumu taip pat buvo klausiama ar jiems yra tekę susidurti su kenkėjiškais laiškais (žr. 14 pav.)



14 pav. Ekspertų nuomonė apie susidūrimą su kenkėjiškais el. laiškais

Vaizdine išraiška pateiktas atsakymas rodo, kad 100 % respondentų, t.y. 9 prokurorai ir 9 karininkai atsakė, kad jiems yra tekę susidurti su kenkėjiškais elektroniniais laiškais. Tai tik patvirtina jau įgytas žinias, kad kenkėjiškų laiškų gavimas yra labai paplitęs.

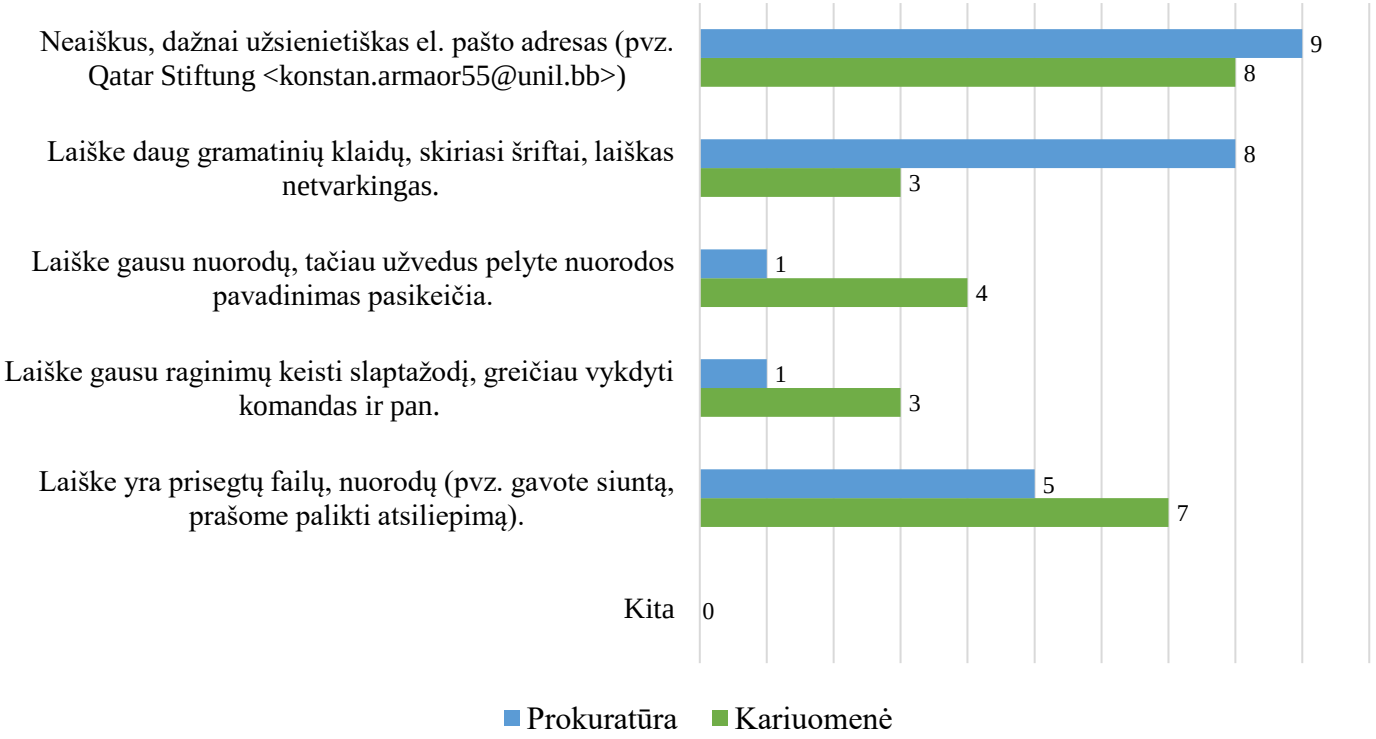
Tam, kad būtų dar aiškiau, ekspertų paklausta ar būtent savo darbiniame elektroniniame pašte yra radę kenkėjiškų laiškų. Atsakymai pavaizduoti skrituline diagrama (žr. 15 pav.):



15 pav. Ekspertų nuomonė apie susidūrimą su kenkėjiškais el. laiškais darbe

Visi tyrimo dalyviai atsakė vienbalsiai, kad visiems yra tekę susidurti su kenkėjiškais elektroniniais laiškais savo darbinėje pašto dėžutėje. Toks vienbalsis respondentų atsakymas tik patvirtina žinias, kad valstybinių įstaigų darbuotojų darbiniai elektroniniai paštai yra aktyviai puldinėjami piktavalių siunčiant kenksmingo pobūdžio elektroninius laiškus.

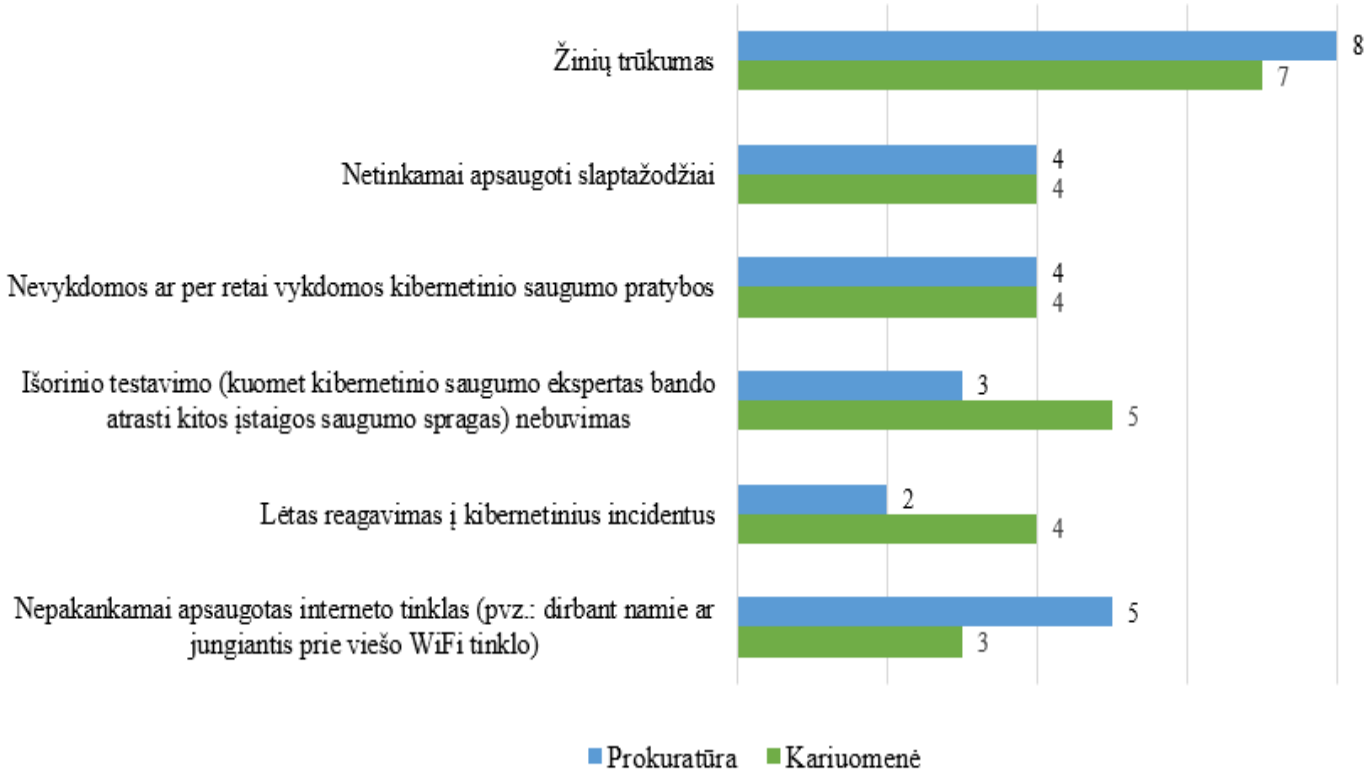
Išsiaiškinus, kad absoliučiai daugumai respondentų yra tekę susidurti su kenkėjiškais el. laiškais svarbu pasitikslinti kokiais bruožais jų nuomone dažniausiai pasižymi tokie laiškai (žr. 16 pav.):



16 pav. Ekspertų nuomonė apie kenkėjiškų laiškų bruožus

Apklausti prokurorai daugiausiai išskyrė tris bruožus: visi 9 prokurorai balsavo, kad kenkėjiški el. laiškai išsiskiria neaiškias, dažniausiai užsienietiškais elektroninio pašto adresais. Taip pat, net 8 prokurorai pažymėjo, kad kenkėjiškame el. laiške dažnai gausu gramatinių klaidų, skiriasi laiško šriftai, jis vizualiai atrodo netvarkingas. Respondentai prokurorai kaip vieną dažniausių bruožų išskyrė, kad laiške gausu nuorodų, prisegtų failų, neteisingos informacijos. Šį atsakymo variantą pasirinko 5 iš 9 prokurorų. Tuos pačius du kaip svarbiausius bruožus išskyrė ir karininkai. 8 pasirinko, kad kenkėjiški laiškai dažnai rašomi iš neaiškių ir užsienietiškų el. paštų bei 7 paminėjo, kad kenkėjiškuose laiškuose gausu prisegtų nuorodų ir failų.

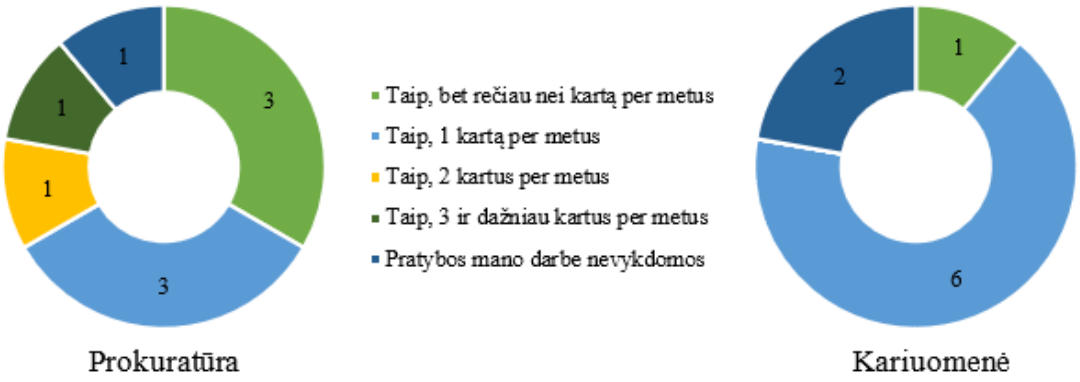
Kitu klausimu siekta išsiaiškinti ekspertų nuomonę apie tai, kokios jų manymu kibernetinio saugumo spragos jų institucijose daro didžiausią žalą. Atsakymai pateikti juostinės diagramos išraiška (žr. 17 pav.):



17 pav. Ekspertų nuomonė apie dažniausias kibernetinio saugumo užtikrinimo problemas

Didžioji dalis prokurorų (8 iš 9 respondentų) pasirinko jog didžiausią neramumą kelia darbuotojų žinių trūkumas kibernetinio saugumo klausimu. Prokurorų manymu, šiai sričiai reikėtų daugiau dėmesio. Tam pritaria ir dauguma karininkų (7 iš 9 respondentų). 5 prokurorai ir tik 3 karininkai kaip vieną didžiausių kibernetinio saugumo grėsmių pasirinko nepakankamai apsaugotus tinklus, kas, remiantis patirtimi ir moksliniais šaltiniais, yra tikrai svarbus saugumo aspektas dirbant iš namų. 5 karininkai ir tik 3 prokurorai išorinio testavimo nebūvimą išskyrė kaip svarbų. Mano nuomone, šį punktą rinkosi mažuma prokurorų, nes galimai neaišku kas yra tas išorinis testavimas arba nežinoma ar jis jų drbovietėje vykdomas. Kaip vidutiniškai svarbius punktus abie respondentų grupės išskyrė netinkamai apsaugotus slaptažodžius ir nevykdomas arba per retai vykdomas kibernetinio saugumo pratybas. Šio punkto mažas interesuotumas parodo, kad respondentai galbūt ne iki galo gerai žino kada ir kokios pratybos jų darbovietėse vykdomos.

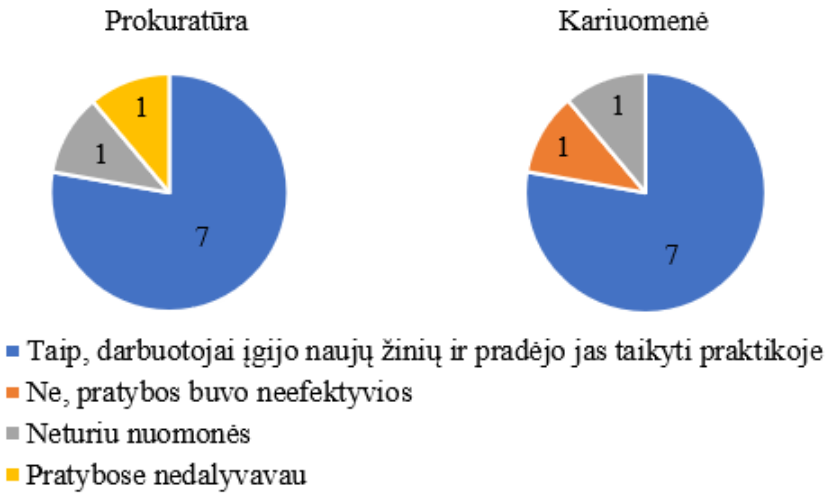
Todėl svarbu išsiaiškinti kokia respondent nuomonė apie kibernetinio saugumo pratybų vykdymo dažnumą jų darbovietėse. Atsakymai pateikiami skritulinių diagram išraiška (žr. 18 pav.):



18 pav. Ekspertų nuomonė apie kibernetinių pratybų dažnumą prokuratūroje ir kariuomenėje

Matoma, kad 3 prokurorai pasirinko jog kibernetinio saugumo pratybos jų darbe vykdomos, bet rečiau nei kartą per metus. Taip pat trys prokurorai rinkosi, kad pratybos vykdomos kartą per metus. Po vieną prokurorą atsakė, kad pratybos vykdomos du kartus, tris kartus per metus. Taip pat vienas prokuroras pasirinko, kad kibernetinio saugumo pratybos jo darbe nėra vykdomos. Tuo tarpu 6 karininkai į tą patį klausimą atsakė, kad KS pratybos kariuomenėje vykdomos kartą per metus. Vienas karininkas atsakė, kad vykdomos rečiau nei kartą per metus. O du karininkai atsakė, kad kibernetinio saugumo pratybos, jų nuomone, kariuomenė iš vis nėra vykdomos. Manau, kad galime daryti išvadą, kad susidomėjimas tokio tipo pratybomis nėra absoliutinis nei vienoje iš tirtų institucijų ir čia yra ta vieta, kurią būtų galima stiprinti ir gerinti.

Svarbu išsiaiškinti respondentų nuomonę apie kibernetinio saugumo pratybų efektyvumą jų darbovietėse (žr. 19 pav.):



19 pav. Ekspertų nuomonė apie kibernetinių pratybų prokuratūroje ir kariuomenėje efektyvumą

7 iš 9 prokurorų pažymėjo, kad pratybos buvo efektyvios ir darbuotojai žinias pradėjo taikyti praktikoje. Vienas prokuroras pažymėjo, kad neturi nuomonės, o kitas, kad pratybose nedalyvavo, todėl atsakyti į klausimą teigiamai ar neigiamai negalėjo. Tuo tarpu taip pat 7 karininkai pažymėjo, kad jų nuomone, vykdytos pratybos davė naudos. Po vieną respondentą pasisakė, kad pratybos buvo neefektyvios ir kad nuomonės apie pratybas neturi. Vertinant pasiskirsčiusius respondentų atsakymus galima teigti, kad dauguma visgi mano, kad pratybos yra naudingos ir jų metu gautas žinias galima panaudoti praktikoje.

Taip pat tyrimo metu buvo svarbu išsiaiškinti ekspertų nuomonę, kaip jų darbovietėje būtų galima stiprinti kibernetinį saugumą (žr. 2 lent.). Ekepertų patarimai patalpinti lentelėje kitame puslapyje:

2 lentelė. Ekspertų patarimai kibernetinio saugumo stiprinimo klausimu prokuratūroje ir kariuomenėje

Prokurorų nuomonė	Karininkų nuomonė
Dažnesnės kibernetinio saugumo pratybos bei pačio vartotojo budrumas, atidumas	KS iškelti kaip prioritetinį klausimą, aktyvūs ir reguliarūs mokymai
Kibernetinio saugumo pratybos, nes vien pateikiama informacija ypatingo efekto nesukelia, dažnai net neįsigilinama.	Naujų saugumo operacijų centrų steigimas daliniuose, naujų etatų atidarymas, didesnės investicijos į kibernetinė saugumą, kursai.
Nuolat domėtis tai, kas vyksta LR visuomenėje, įskaitant ir pasaulinę, ir daryti asmenines išvadas, sąlygojančias tavo asmeninį ir šeimyninį gyvenimą.	Daigiau informacijos apie kibernetinį saugumą, paskaitos, pratybos.
Budrumas	Būti budresniems
Žmonių pastovus švietimas kibernetinio saugumo klausimais	Mokymai darbuotojams kibernetinio saugumo klausimais
Dažnesnės pratybos	Žmogiškieji ištekliai, naujausios technologijos, švietimas.
Informacija su pateiktais laiškų pavyzdžiais	Daugiau dėmesio darbuotojų švietimui KS klausimais
Neturiu nuomonės.	Neaktualu

Susisteminus lentelės duomenis galime daryti išvadą, kad dauguma prokurorų patarė daryti dažnesnes pratybas, taip pat akcentuoti darbuotojų švietimą bei budrumą. Prokurorų nuomone, kad svarbu nuolat domėtis kas vyksta LR visuomenėje, pasaulyje bei daryti išvadas. Pastovus švietimas ir tobulėjimas, prokurorų nuomone, būtų efektyvus žingsnis tobulinant kibernetinį saugumą prokuratūroje.

Tuo tarpu karininkai taip pat švietimą kibernetinio saugumo klausimais, reguliarius mokymus bei pratybas taip pat iškėlė kaip gerus būdus stiprinti kibernetinį saugumą kariuomenėje. Karininkų nuomone taip pat svarbu būti budriems, daugiau dėmesio skirti žmogiškiesiems ištekliams ir kibernetinį saugumą iškelti kaip prioritetinį klausimą. Didesnės investicijos ir naujų operacijų centrų bei etatų kūrimas taip pat pagelbėtų sėkmingam kibernetinio saugumo užtikrinimui kariuomenėje.

IŠVADOS IR REKOMENDACIJOS

1. Išanalizavus elektroninės valdžios sistemas, atlikus mokslinių šaltinių analizę atskleisti trys pagrindiniai elektroninės valdžios diegimo modeliai pagal vartotojų grupes: valdžia - gyventojams (G2C); valdžia - valdžiai (G2G); valdžia - verslui (G2B). Išsiaiškinta, kad valdžia - valdžiai modelis daugeliu atžvilgių yra elektroninės valdžios pagrindas, ir valdžia, norėdama sėkmingos elektroninės komunikacijos su piliečiais, pirmiausia turi tobulinti ir modernizuoti savo vidaus sistemą bei procedūras.

2. Atlikus pasaulinę elektroninės valdžios kūrimo ir diegimo analizę pastebėta, kad Lietuva pagal elektroninės valdžios raidos indeksą yra aktyviai tobulėjanti šalis- iš 40 pozicijos 2018 metais pakilo į 24 poziciją 2020 metais. Taip pat Lietuva 2018 metais pateko į 11 šalių, teikia aukštos kokybės skaitmenines paslaugas, sąrašą. Atlikta pasaulinės patirties lyginamoji analizė parodė, kad Lietuvos pozicija kibernetinio saugumo kontekste yra kylanti ir akcentavus reikiamus taškus galime tarpti kibernetiškai stipria valstybe.

3. Išnagrinėti kibernetinį saugumą užtikrinančios institucijos ir išsiaiškinta, kad svarbiausią funkciją atlieka LR Vyriausybė, kuri nubrėžia šalies kibernetinio saugumo politikos gaires tvirtindama ilgalaikius planus ar programas. Krašto apsaugos ministerija ir Kibernetinio saugumo taryba rengia Kibernetinio saugumo sritį reguliuojančius teisės aktus, pavyzdžiui, Kibernetinio saugumo įstatymą. Krašto apsaugos ministerijos parengtų teisės aktų įgyvendinimą užtikrina Nacionalinis kibernetinio saugumo centras, Lietuvos policija ir Valstybinė duomenų apsaugos inspekcija. Kibernetinio saugumo subjektai yra Lietuvoje veikiančios valstybės institucijos ir privačios organizacijos. Jos privalo įgyvendinti kibernetinio saugumo teisės aktų reikalavimus. Kibernetiniam saugumui didžiausią pavojų kelia kibernetinių atakų vektoriai. Per 2020 m. balandžio mėnesio iki 2021 m. liepos mėnesio laikotarpį šalyje labiausiai nukentėjo vyriausybinis viešojo administravimo sektorius. Siekiant išvengti kibernetinių atakų svarbu žinoti saugumo stiprinimo būdus: Informacijos šifravimas ir atsarginių kopijų kūrimas; Reguliarus darbuotojų mokymas; Kelių lygių autentifikavimas; Reguliarus programinės įrangos ir sistemų atnaujinimas.

4. Atlikti elektroninės valdžios sistemų tobulinimo nacionalinio kibernetinio saugumo kontekste kokybinį tyrimą prokuratūroje kariuomenėje, išsiaiškinta, kad nors apklaustų ekspertų kibernetinio saugumo žinios gana geros, tačiau kibernetinio saugumo klausimo svarba valstybinėse institucijose dar yra nepakankamai prioritetinis klausimas. Remiantis ekspertų nuomone galima teigti, kad norint didinti darbuotojų žinias apie kibernetinį saugumą reikia skirti daugiau finansavimo, vykdyti dažnesnius mokymus ir pratybas.

Rekomendacijos:

- Kuo daugiau remtis kitų Europos ar pasaulio šalių gerąja praktika elektroninės valdžios vystymosi klausimais.
- Diegiant elektroninės valdžios sistemų atnaujinimą remtis sėkminga Danijos Karalystės ir Naujosios Zelandijos patirtimi.
- Kibernetinio saugumo užtikrinimo klausimą išskirti kaip vieną iš prioritetinių, ypatingai kalbant apie valstybinių įstaigų kibernetinį saugumą.
- Reguliariai vykdyti kibernetinio saugumo pratybas valstybinio sektoriaus įstaigose ir vėliau pateikti išsamias ataskaitas darbuotojams ir visuomenei apie pratybų efektyvumą.
- Vykdyti išorinį valstybinių įstaigų testavimą.
- Formuoti kibernetinių grėsmių analizės mechanizmus valstybės mastu, kurie padėtų prognozuoti potencialias grėsmes ir atsižvelgiant į gautą informaciją aktyviai formuoti kibernetinės gynybos elementus.
- Pateikti gaires kaip būtų galima apsaugoti labiausiai pažeidžiamus objektus organizacijose bei institucijose nuo kibernetinių pažeidimų.
- Steigti naujus saugumo operacijos centrus, didinti kibernetinių ekspertų darbo vietų skaičių, ypač valstybinėse institucijose.
- Atkreipti didesnį dėmesį į geopolitines aplinkybes ir aktyviai diegti informacijos vertinimo mechanizmus, kurie būtų skirti stebėti geopolitinę situaciją iš kibernetinio saugumo perspektyvos.

LITERATŪROS SĄRAŠAS

Teisės aktai ir dokumentai:

1. European Commission. (2022). Shaping Europe's digital future. Prieiga per internetą: https://digital-strategy.ec.europa.eu/en/policies/discover-eidas;
2. Europos Komisija. (2018). e-Government Benchmark 2018: the digital efforts of European countries are visibly paying off. *Shaping Europe's digital future.* Prieiga per internetą:https://digital-strategy.ec.europa.eu/en/news/egovernment-benchmark-2018-digital-efforts-european-countries-are-visibly-paying;
3. Europos Komisija. (2019). E-Government factsheets anniversary report. Prieiga per internetą: https://ec.europa.eu/isa2/sites/default/files/docs/news/10egov_anniv_report.pdf;
4. Europos Komisija. (2020). The EC reveals its new EU Action Plan on Integration and Inclusion (2021-2027). Prieiga per internetą:https://ec.europa.eu/migrant-integration/news/ec-reveals-its-new-eu-action-plan-integration-and-inclusion-2021-2027_en;
5. Europos Komisija. (2022). Communication From The Commission To The European Parliament And The Council on the Fourth Progress Report on the implementation of the EU Security Union Strategy. Prieiga per internetą: https://ec.europa.eu/info/sites/default/files/communication_fourth_progress_report-eu_security_union_strategy.pdf;
6. Europos Komisija.(2016). Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=LEGISSUM:4301896;
7. Europos Parlamentas (2022). Cybersecurity: Main And Emerging Threats In 2021 (Infographic). Prieiga per internetą: https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats-in-2021-infographic#ssh_slides;
8. Europos Parlamentas ir Europos Sąjungos taryba, (2014). Reglamentas (ES) Nr. 910/2014 2014 m. liepos 23 d. dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB. Prieiga per internetą:https://eur-lex.europa.eu/legalcontent/LT/TXT/?uri=CELEX%3A32014R0910&qid=1623231710001;

9. Jungtinių Tautų elektroninės valdžios plėtros duomenų bazė (United Nations E-Government Development Database (2022). Prieiga per internetą:https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index;
10. Krašto apsaugos ministerija. (2018). Nacionalinė kibernetinio saugumo strategija. PATVIRTINTA Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818. Priega per internetą: https://kam.lt/wp-content/uploads/2022/03/nacionaline-kibernetinio-saugumo-strategija.pdf;
11. Lietuvos Respublikos baudžiamojo kodekso 198 straipsnis 2007 06 28 įstatymu Nr. X-1233 (nuo 2007 07 21), (Žin., 2007, Nr. 81-3309). Prieiga per internetą: http://www.infolex.lt/ta/66150:str198;
12. Lietuvos Respublikos kibernetinio saugumo įstatymas. 2014 m. Gruodžio 11 d. Nr. XII-1428. Teisės aktų registras. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4;
13. Viešųjų paslaugų teikiamų informacinėmis technologijomis esamos būklės analizė (2008). Lietuvos Respublikos vidaus reikalų ministerija, Socialinės ekonominės plėtros centras.

Vadovėliai ir monografijos:

14. Alshomrani, S., Qamar, S., (2013). Cloud Based E-Government: Benefits and Challenges. International Journal of Multidisciplinary Sciences and Engineering, 4(6), 1-7;
15. Augustinaitis, A, Rudzikienė, V., Petrauskas, R. A., Dagytė, I., Martinaitytė, E., Leichteris, E., Malinauskienė, E., Višnevska, V., Žilionienė, I. (2009). Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas. Kolektyvinė monografija. Vilnius. Mykolo Riomerio Universitetas. Prieiga per internetą:https://repository.mruni.eu/bitstream/handle/007/16745/9789955192510.pdf?sequence=1&isAllowed=y;
16. Baležentis A., Žalimaitė M. (2011). Ekspertinių vertinimų taikymas inovacijų plėtros veiksnių analizėje: Lietuvos inovatyvių įmonių vertinimas. Vadybos mokslas ir studijos – kaimo verslų ir jų infrastruktūros plėtrai, Nr. 3 (27), P. 23-31.;
17. Bansal, K. L., Sharma, S. K., & Sood, S., 2012. Impact of Cloud Computing in Implementing Cost Effective E-governance Operations. *GIAN JYOTI E-JOURNAL*, 1(2);
18. Caves, R.W. (2005). *Encyclopedia of the City*. Nuoroda per internetą: https://shora.tabriz.ir/Uploads/83/cms/user/File/657/E_Book/Urban%20Studies/Encyclopedia%20of%20the%20City.pdf;

19. Chadwich, A., Stromer-Galley, J. (2016). *Digital Media, Power, and Democracy in Parties and Election Campaigns: Party Decline or Party Renewal?* Prieiga per internetą: https://doi.org/10.1177%2F1940161216646731
20. Garuckas R., Kaziliūnas A. (2008). E. valdžios ir viešojo sektoriaus sąveikos Lietuvoje analizė// Viešoji politika ir administravimas. 2008, Nr.23. 60 p.;
21. Kardelis, K. (2002). Mokslinių tyrimų metodologija ir metodai. 2-asis pataisytas ir papildytas leidimas. Kaunas;
22. Padallan, J. O. (2019). Cyber Security. Arcler Press. Prieiga per internetą: https://web-p-ebscohostcom.skaitykla.mruni.eu/ehost/ebookviewer/ebook/bmxlYmtfXzIzMjQzMjdfX0FO0?sid=1756276f-f6be-4f9d-8c0a-69bb7e3f3566@redis&vid=3&format=EB&rid=4;
23. Tidikis, R. (2003). Socialinių mokslų tyrimų metodologija. Vilnius: Lietuvos teisės universiteto leidybos centras.

Kiti moksliniai šaltiniai:

24. Bansal, K. L., Sharma, S. K., & Sood, S., 2012. Impact of Cloud Computing in Implementing Cost Effective E-governance Operations. *GIAN JYOTI E-JOURNAL*, 1(2);
25. Barker, S. (2021). The Who's Who Of NZ's Government & Public Cybersecurity Agencies. Prieiga per internetą: https://securitybrief.co.nz/story/the-who-s-who-of-nz-s-government-public-cybersecurity-agencies;
26. Butler, T., Feller, J., Pope, A., Barry, P., Murphy, C. (2005). Promoting knowledge sharing in government and non-government organizations using open source software. Academic *Conferences,Ltd.* Prieiga per internetą:https://academic-publishing.org/index.php/ejeg/article/view/409/372;
27. Caves, R.W. (2005). *Encyclopedia of the City.* Nuoroda per internetą: https://shora.tabriz.ir/Uploads/83/cms/user/File/657/E_Book/Urban%20Studies/Encyclopedia%20of%20the%20City.pdf;
28. Chadwich, A., Stromer-Galley, J. (2016). *Digital Media, Power, and Democracy in Parties and Election Campaigns: Party Decline or Party Renewal?* Prieiga per internetą: https://doi.org/10.1177%2F1940161216646731
29. Chaudharya, P., Gupta, B. B., Chang, X., Nedjah, N., Tai Chui, K. (2021). Enhancing Big Data Security Through Integrating XSS Scanner Into Fog Nodes For Smes Gai. *Technological Forecasting and Social Change,* Volume 168. Prieiga per

internetą:https://www.sciencedirect.com/science/article/abs/pii/S0040162521001864?via%3Dihub;

30. Chebac, A. (2022). Becoming the Most Cyber-Secure Country. Is IT Security are big enough political topic for Danes? Prieiga per internetą: https://heimdalsecurity.com/blog/denmarks-cybersecurity-journey-to-becoming-the-most-cyber-secure-country/;
31. Fathey, M., Othman, I. (2016). Models Of Adopting Cloud Computing In The E-Government Context: A Review. Jurnal Teknologi, vol 73, p. 51-59. Prieiga per internetą:https://www.researchgate.net/publication/304370164_Cloud_computing_adoption_model_for_e-government_implementation;
32. Ghaffar, H.A.N.A. (2020). Government Cloud Computing and National Security. Prieiga per internetą:https://www.emerald.com/insight/content/doi/10.1108/REPS-09-2019-0125/full/pdf;
33. Hartley, D. (2012). SQL Injection Attacks and Defense. What Is SQL Injection? Prieiga per internetą: https://www.sciencedirect.com/sdfe/pdf/download/eid/3-s2.0-B9781597499637000013/first-page-pdf;
34. Yadav, N., Singh, V.B. (2012). E-Governance: Past, Present and Future in India. *International Journal of Computer Applications (0975 – 8887) Volume 53– No.7*. .Prieiga per internetą: https://arxiv.org/ftp/arxiv/papers/1308/1308.3323.pdf
35. Kiškis, M., Limba, T. (2004). Elektroninės valdžios teisinio reglamentavimo prielaidos: esamų iniciatyvų Lietuvoje analizė. *Jurisprudencija.* 2004, Nr. 57-49.;
36. Kundra, V. (2011) Federal Cloud Computing Strategy. Office of Management and Budget, Office of E-Government and Information Technology, Washington DC.
37. Liang, J., (2012). Government cloud: enhancing efficiency of e-government and providing better public services. Paper presented at the Service sciences (IJCSS), 2012 international joint conference on;
38. Maji, S.,Jain, H., Pandey, V.,Siddiqui, V. A.(2022). White Hat Security-An Overview of Penetration Testing Tools. *Proceedings of the Advancement in Electronics & Communication Engineering.* Prieiga per internetą: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4159095;
39. McGuinness, D. (2017). How a cyber attack transformed Estonia. Prieiga per internetą: https://www.bbc.com/news/39655415;
40. Nur, W.H., Narulita, I., Kumoro, Y., Susilowati, Y., Yuliana, Y., Fajary, F. R., Wulandari, S. N. (2022). A cloud GIS-based framework implementation in developing countries. *Bulletin of Electrical Engineering and Informatics* 11(4):2243-2252 Priega per internetą:

https://www.researchgate.net/publication/362397672_A_cloud_GISbased_framework_implementation_in_developing_countries;

41. Patrascu, P. (2018). The Appearance and Development of National Cyber Security Strategies. *The 14 th International Scientific Conference eLearning and Software for Education Bucharest*. Prieiga per internetą:https://www.ceeol.com/search/article-detail?id=669394;
42. Pauli, J. (2013). The Basics of Web Hacking. Tools and Techniques to Attack the Web Prieiga per internetą: https://www.sciencedirect.com/topics/computer-science/injectionvulnerability;
43. Sear, M. J. (2021). The Digital Government of New Zealand: Striving for Efficiency and Innovation. Prieiga per internetą: https://www.linkedin.com/pulse/digital-government-new-zealand-striving-efficiency-innovation-sear/?trk=public_profile_article_view;
44. Shema, M. (2010). Seven Deadliest Web Application Attacks. Breaking Authentication Schemes. Prieiga per internetą: https://www.sciencedirect.com/book/9781597495431/sevendeadliest-web-application-attack;
45. Sahu, B. L., Tiwari, R. (2012). A comprehensive study on Cloud computing. International journal of Advanced Research in Computer science and Software engineering, 2(9);
46. Sukianto, A. (2022). 10 Ways to Reduce Cybersecurity Risk for Your Organization. *Third-Party Risk Management*. Prieiga per internetą: https://www.upguard.com/blog/reduce-cybersecurity-risk;
47. Tahirkheli, A. I., Shiraz, M.,Hayat, B.,Idrees, M.,Sajid, A.,Ullah, R.,Ayub, N., Kim, K. (2021). A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. *Digital Object Identifier 10.1109/ACCESS.2021.3073203.* Prieiga per internetą: https://www.mdpi.com/2079-9292/10/15/1811;
48. Van der Meuler. (2018).Understanding cloud adoption in govern Gartner. *Sensor Networks*;
49. Sun, Y., Zhang, J., Xiong,Y., Zhu, G. (2014).Data security and privacy in cloud computing, *International Journal of Distributed; doi: 10.1155/2014/19090;*
50. Venkina, E. (2021). How Denmark Became The Most Cyber-Secure Country. Prieiga per internetą: https://www.ips-journal.eu/work-and-digitalisation/how-denmark-became-the-most-cyber-secure-country-5290/.

Žiniasklaidos šaltiniai:

51. BNS (2010, liepos 10d.). Registrų centras, „Sodra“ ir VMI uždraudė prisijungimą per Elektroninės valdžios vartus. Kauno diena. Prieiga per internetą:

https://kauno.diena.lt/naujienos/salies-pulsas/registru-centras-sodra-ir-vmi-uzdraudeprisijungima-elektronines-valdzios;

52. Europos Sąjungos leidinių biuras. (2016). Saugesnės operacijos internetu. Prieiga per internetą:https://eur-lex.europa.eu/legal-content/LT/LSU/?uri=CELEX:02014R0910-20140917;
53. E-valdžios sąveikumo portalas. E- valdžios samprata. Prieiga per internetą: http://saveikumas.gov.lt/lt/saveikumas/e.-valdzios-samprata.html;
54. Informacinės visuomenės plėtros komitetas, (2018). VIISP. Prieiga per internetą:https://ivpk.lrv.lt/lt/struktura-ir-kontaktai/vadovai/ivpk/lt/veikla/veiklos-sritys/viisp;
55. Jackevičius, M. (2010). IT specialistai dėl sistemos spragų gali prisijungti ir prie jūsų SoDros duomenų. *Delfi technologijos ir mokslas.* 2010 m. liepos 10d. Prieiga per internetą: https://www.delfi.lt/mokslas/technologijos/it-specialistas-del-sistemos-spragu-galiuprisijungti-ir-prie-jusu-sodros-duomenu.d?id=34329025;
56. Jungtinių Tautų elektroninės valdžios plėtros duomenų bazė (United Nations E-Government Development Database (2022). Prieiga per internetą:https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index;
57. LDM filialo LM ISC LIMIS informacija (2018, kovo 9d). Elektroniniai valdžios vartai. Kas tai? Prieiga per internetą: http://www.ekultura.lt/elektroniniai-valdzios-vartai-kas-tai/;
58. Lietuvos Respublikos ryšių reguliavimo tarnyba, (2020). Kas yra dviejų faktorių autentifikacija? Prieiga per internetą: https://esaugumas.lt/naujienos/kas-yra-dvieju-faktoriuautentifikacija;
59. Lietuvos Respublikos ryšių reguliavimo tarnyba, (2020). Phishing. Kaip apsaugoti savo duomenis? Prieiga per internetą: https://esaugumas.lt/news/phishing-kaip-apsaugoti-savoduomenis;
60. Lietuvos Respublikos Seimo kanceliarija. (2021). Viešojo administravimo sistemos Europos Sąjungos valstybėse narėse: valstybės tarnybų modeliai, skaitmenizavimo iššūkiai, viešojo sektoriaus dydžio ir efektyvumo koreliacijos su valstybės perskirstomuoju vaidmeniu. *Analitinė apžvalga 21/42.* Prieiga per internetą: https://www.lrs.lt/sip/getFile3?p_fid=32865;
61. Lietuvos Respublikos vidaus reikalų ministerija, (2020). Elektroninio parašo sukūrimas. Prieiga per internetą: https://eid.lt/lt/apie-tapatybes-kortele/elektroninio-paraso-sukurimas;
62. Lietuvos statistika. Elektroniniai valdžios vartai. Prieiga per internetą: https://www.stat.gov.lt/elektroniniai-valdzios-vartai;
63. LR Krašto apsaugos ministerija. (2022). Kibernetinio saugumo mėnuo. Prieiga per internetą: https://kam.lt/kibernetinio-saugumo-menuo-2022/;

64. LR Prokuratūra (2019, birželio 10d.) Nusikaltimai elektroninėje erdvėje. Prieiga per internetą:https://www.prokuraturos.lt/lt/veiklos-sritys/baudziamasispersekiojimas/nusikaltimai-elektronineje-erdveje/185;
65. Lrt.lt (2021, kovo 31d.), Vyriausybė pritarė įstatymo pataisoms, padėsiančioms kurti saugesnę kibernetinę erdvę. Prieiga per internetą: https://www.lrt.lt/naujienos/lietuvoje/2/1377488/vyriausybe-pritare-istatymo-pataisomspadesiancioms-kurti-saugesne-kibernetine-erdve;
66. Nacionalinės statistikos biuras. (2022). Phishing attacks – who is most at risk? Prieiga per internetą:https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/phishingattackswhoismostatrisk/2022-09-26;
67. NKSC (2017). Nacionalinio kibernetinio saugumo būklės ataskaita už 2017 metus. Prieiga per internetą: https://www.nksc.lt/doc/NKSC_ataskaita_2017_lt.pdf;
68. Skaitmeninės valdžios agentūra. Borger.dk – National Citizen Portal. Prieiga per internetą: https://en.digst.dk/digital-services/borgerdk-national-citizen-portal/my-overview/;
69. Skersys, G. (2011). Informacijos sauga. Prieiga per internetą: http://www.esparama.lt/documents/10157/490675/Informacijos_sauga.pdf/135c8158-3957-40b0-a5a9-e0fa17e364dd;
70. Viešųjų paslaugų teikiamų informacinėmis technologijomis esamos būklės analizė (2008). Lietuvos Respublikos vidaus reikalų ministerija, Socialinės ekonominės plėtros centras.

Petkevičiūtė V. (2022). E. Valdžios sistemų tobulinimas nacionalinio kibernetinio saugumo kontekste: pasaulinė patirtis ir Lietuvos perspektyva (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas.

ANOTACIJA

Magistriniame baigiamajame darbe analizuojamos e. valdžios sistemos, jos tobulinimo galimybės kibernetinio saugumo kontekste. Atlikta pasaulinės patirties lyginamoji analizė parodė, kad Lietuvos pozicija kibernetinio saugumo kontekste yra kylanti ir akcentavus reikiamus taškus galime tarpti kibernetiškai stipria valstybe. Pirmoje darbo dalyje nagrinėjami elektroninės valdžios teoriniai aspektai: elektroninės valdžios samprata, e. valdžia Lietuvoje ir elektroniniai valdžios vartai. Antroje dalyje analizuojamas elektroninės valdžios sistemų vystymas ir įgyvendinimas pasaulyje bei Europoje, Jungtinių Tautų elektroninės valdžios raidos indeksas, elektroninės valdžios tobulinimas. Pateikiama lyginamoji analizė- Danijos Karalystės ir Naujosios Zelandijos pavyzdžiai bei Lietuvos situacija pasaulio ir ES kibernetinio saugumo kontekste. Trečioje dalyje nagrinėjama Lietuvos kibernetinio saugumo architektūra, saugumo pažeidimai, labiausiai pažeidžiami sektoriai bei kibernetinio saugumo pažeidimai valstybinėse įstaigose. Ketvirtoje dalyje nagrinėjamas atliktas tyrimas, kurio tikslas - pasitelkiant ekspertų žinias, išsiaiškinti kaip dažnai prokuratūroje ir kariuomenėje atliekamos kibernetinio saugumo pratybos, ar darbuotojai tiesiogiai susiduria su kibernetinėmis grėsmėmis ir ar jiems žinoma ką daryti pastebėjus kibernetinį nusikaltimą jų darbovietėje.

Pagrindiniai žodžiai: elektroninė valdžia, elektroniniai valdžios vartai, kibernetinis saugumas, pasaulinė patirtis ir Lietuvos perspektyva.

Petkevičiūtė V. (2022). E- Government Systems Improvement in the Context Of National Cyber Security: Global Experience and Prospect in Lithuania (master thesis). Vilnius: Mykolas Romeris University.

ANNOTATION

In Master‘s thesis analyzed e. government system, its improvement possibilities in the context of cyber security. The comparative analysis of global experience has shown that Lithuania's position in the context of cyber security is rising and by emphasizing the necessary points, we can become a strong country in cyber security. The first part of the work examines the theoretical aspects of electronic government: the concept of electronic government, e. government in Lithuania and the electronic government portal. The second part analyzes the development and implementation of electronic government systems in the world and in Europe, the United Nations electronic government development index, and the improvement of electronic government. A comparative analysis is presented - the examples of the Kingdom of Denmark and New Zealand and the situation of Lithuania in the context of global and EU cyber security. The third part examines the Lithuanian cyber security architecture, security breaches, the most vulnerable sectors and cyber security breaches in state institutions. The fourth part examines the conducted research, the purpose of which is to find out, using the knowledge of experts, how often cyber security exercises are carried out in the prosecutor's office and the army, whether employees are directly exposed to cyber threats and whether they know what to do if they notice a cyber crime in their workplace.

Key words: electronic government, electronic government gateway, cyber security, global experience and Lithuania's perspective.

Petkevičiūtė V. E. valdžios sistemų tobulinimas nacionalinio kibernetinio saugumo kontekste: pasaulinė patirtis ir Lietuvos perspektyva / Kibernetinio saugumo valdymo magistro baigiamasis darbas. Vadovas prof. dr. T. Limba. – Vilnius: Mykolo Romerio universitetas, Viešojo valdymo ir verslo fakultetas, 2022. – 80 p.

SANTRAUKA

Magistro baigiamojo darbo tikslas – remiantis literatūra bei teisiniais dokumentais, išanalizuoti elektroninės valdžios tobulinimo galimybes Lietuvoje ir atskleisti kaip užtikrinamas šalies elektroninių valdžios vartų kibernetinis saugumas bei pateikti su šia sritimi susijusias rekomendacijas ir pasiūlymus.

Augant viešųjų ir administracinių elektroninių paslaugų skaičiui, didėja ir kibernetinių atakų tikimybė. Pagal 2020 metų ataskaitą, kibernetinių nusikaltimų skaičius išaugo 25%. Prie kibernetinių nusikaltimų suaktyvėjimo prisidėjo ir COVID- 19 pandemija, nes daugeliui darbuotojų pradėjus dirbti iš namų, nusikaltėliams pažeisti jų privatumą kibernetinėje erdvėje tapo dar lengviau. Magistriniame darbe, remiantis pasauline analize ir kokybiniu tyrimu atliktu Lietuvoje valstybinėse institucijose, bus aptartas mažai analizuotas klausimas – viešojo kibernetinio saugumo spragos.

Darbe taikyta mokslinės literatūros ir dokumentų turinio, teisės aktų analizė bei atlikta dviejų susijusių grupių ekspertų apklausa. Magistriniame darbe siekiant išsiaiškinti teorinius elektroninės valdžios kūrimo, vystymosi, įgyvendinimo ir tobulinimo aspektus buvo taikyta mokslinės literatūros analizė. Statistinių duomenų analizės metodas buvo taikomas siekiant išskirti dvi šalis atvejo analizei. Buvo pasirinktos dvi šalys: viena Europos Sąjungos šalis (Danija) ir viena Okeanijos regiono šalis (Naujoji Zelandija), kurių gerąją kibernetinio saugumo kūrimo ir tobulinimo praktiką būtų galima pritaikyti Lietuvoje. Pasirinkus atvejo analizės metodą siekta išskirti atrinktų šalių elektroninės valdžios praktikos pritaikomumą Lietuvoje. Taip pat siekiant išsiaiškinti įvairių grupių (prokurorų bei karininkų) nuomonę, atliktas kokybinis tyrimas. Tyrimu siekta išsiaiškinti su kokiomis kibernetinio saugumo problemomis susiduria valstybinio sektoriaus darbuotojai.

Magistro darbą sudaro 4 dalys. Pirmoje darbo dalyje nagrinėjami elektroninės valdžios teoriniai aspektai. Antroje dalyje analizuojamas elektroninės valdžios sistemų vystymas ir įgyvendinimas pasaulyje bei Europoje, Jungtinių Tautų elektroninės valdžios raidos indeksas, elektroninės valdžios tobulinimas. Pateikiama lyginamoji analizė bei Lietuvos situacija pasaulio ir ES kibernetinio saugumo kontekste. Trečioje dalyje nagrinėjama Lietuvos kibernetinio saugumo architektūra, labiausiai pažeidžiami sektoriai bei kibernetinio saugumo pažeidimai valstybinėse įstaigose. Ketvirtoje dalyje nagrinėjamas atliktas tyrimas, kurio tikslas- išsiaiškinti kaip dažnai valstybinėse įstaigose atliekamos kibernetinio saugumo pratybos, ar darbuotojai tiesiogiai susiduria su grėsmėmis ir ar jiems žinoma ką daryti pastebėjus kibernetinį nusikaltimą jų darbovietėje.

Petkevičiūtė V. E- government Systems Improvement in the Context Of National Cyber Security: Global Experience and Prospect in Lithuania / Master thesis in Cyber Security Management. Supervisor assoc. prof. dr. T. Limba. – Vilnius: Faculty of Public Management and Business, Mykolas Romeris University, 2022. – 80 p.

SUMMARY

The aim of the master degree thesis is to analyze the possibilities of improvement of electronic government in Lithuania on the basis of literature and legal documents and to reveal how the cyber security of the country's electronic government portal is ensured and to present recommendations and proposals related to this area.

As the number of public and administrative electronic services grows, so does the probability of cyber attacks. According to the 2020 report, the number of cyber crimes increased by 25%. The COVID-19 pandemic also contributed to the intensification of cybercrime, as many employees started working from home, making it even easier for criminals to violate their privacy in cyberspace. In the master's thesis, based on a global analysis and a qualitative study conducted in Lithuanian state institutions, we barely analyzed the issue of public cyber security gaps.

In this work we used the analysis of the content of scientific literature and documents, legal acts, and conducted a survey of experts from two related groups. In order to find out the theoretical aspects of the creation, development, implementation and improvement of electronic government, an analysis of scientific literature was used in the master's thesis. A statistical data analysis method was applied to identify two countries for case analysis. Two countries were chosen: one country of the European Union (Denmark) and one country of the Oceania region (New Zealand), whose good practices of creating and improving cyber security could be applied in Lithuania. By choosing the case analysis method, the aim was to distinguish the applicability of the electronic government practices of the selected countries in Lithuania. Also, in order to find out the opinion of various groups (prosecutors and officers), a qualitative study was conducted. The research aimed to find out what cyber security problems public sector employees face.

A Master‘s degree is made from 4 parts. First part explores theoretical aspects of electronic government. Second part analyzes electronic government system development and implementation globally also Europe wide and United Nation e-government development A comparative analysis and the situation of Lithuania in the context of global and EU cyber security are presented. The third part examines the cyber security architecture of Lithuania, the most vulnerable sectors and cyber security violations in state institutions. The fourth part examines the conducted research, the purpose of which is to find out, using the knowledge of experts, how often cyber security exercises are carried out in the

prosecutor's office and the army, whether employees are directly exposed to cyber threats and whether they know what to do if they notice a cyber crime in their workplace.

2 PRIEDAS. EKSPERTŲ APKLAUSA

Kibernetinis saugumas valstybinėse institucijose

Laba diena, gerbiamas (-a) respondente, esu Mykolo Romerio Universiteto, Kibernetinio saugumo valdymo studijų programos magistrantė Viltė Petkevičiūtė. Šia anketa norima sužinoti Jūsų nuomonę kibernetinio saugumo klausimu Jūsų darbovietėje (jūsų atsakymai bus pateikiami tik kaip asmeninė nuomonė, o ne visos įstaigos pozicija). Surinkti duomenys bus statistiškai apibendrinami ir naudojami rengiant mokslines išvadas bei praktines rekomendacijas magistro darbe.

Dėkoju už Jūsų skirtą laiką ir įžvalgas!

Esant poreikiui su manimi galite susisiekti el. paštu: vilte.petkeviciute@gmail.com

1. Jūsų darbovietė?

Pažymėkite tik vieną.

- o Prokuratūra
- o Kariuomenė

2. Kiek ilgai dirbate savo darbovietėje?

Pažymėkite tik vieną.

- o Iki vienerių metų.
- o 1 - 3 metus
- o 3 - 5 metus
- o 5 - 10 metų
- o 10 - 15 metų
- o 15 metų ir daugiau

3. Kaip manote, ar kibernetinio saugumo užtikrinimas Jūsų darbe yra svarbus aspektas? *Pažymėkite tik vieną.*

- o Taip, svarbus.
- o Ne, nesvarbus.
- o Neturiu nuomonės

4. Kaip manote, ar kibernetinio saugumo užtikrinimui Jūsų darbovietėje yra skiriama pakankamai daug dėmesio? *Pažymėkite tik vieną.*

- ○ Taip, skiriama daug dėmesio.
- ○ Ne, reikėtų daugiau.
- ○ Neturiu nuomonės, nesidomiu kibernetinio saugumo aspektu.

5. Ar žinote į ką galima kreiptis pastebėjus kibernetinio saugumo pažeidimą? *Pažymėkite tik vieną.*

- ○ Taip.
- ○ Ne.
- ○ Nesu tikras (-a).

6. Ar teko susidurti su kenkėjiškais laiškais? *Pažymėkite tik vieną.*

- ○ Taip, ne kartą.
- ○ Neteko.
- ○ Nežinau kas yra kenkėjiškas laiškas

7. Ar į savo darbinį el. paštą esate gavę kenkėjiškų laiškų? *Pažymėkite tik vieną.*

- ○ Taip.
- ○ Ne.
- ○ Nežinau arba nepamenu.

8. Ar galėtumėte įvardinti kokiais bruožais, Jūsų nuomone, išsiskiria kenkėjiškas laiškas? *Galimi keli atsakymo variantai*

- □ Neaiškus, dažnai užsienietiškas el. pašto adresas (pvz. Qatar Stiftung <k onstan.armaor55@unil.bb>)
- □ Laiške daug gramatinių klaidų, skiriasi šriftai, laiškas netvarkingas.

- Laiške gausu nuorodų, tačiau užvedus pelyte nuorodos pavadinimas pasikeičia.
- Laiške gausu raginimų keisti slaptažodį, greičiau vykdyti komandas ir pan. gavote siuntą, prašome palikti atsiliepimą).
- Kita (įrašykite)

9.Kaip manote, kokios problemos kelia didžiausius sunkumus sklandžiam kibernetinio saugumo užtikrinimui?

Galimi keli atsakymo variantai.

- Žinių trūkumas
- Netinkamai apsaugoti slaptažodžiai
- Nevykdomos ar per retai vykdomos kibernetinio saugumo pratybos
- Išorinio testavimo (kuomet kibernetinio saugumo ekspertas bando atrasti kitos įstaigos saugumo spragas) nebuvimas
- Lėtas reagavimas į kibernetinius incidentus
- Nepakankamai apsaugotas interneto tinklas (pvz.: dirbant namie ar jungiantis prie viešo WiFi tinklo)
- Kita(įrašykite)

10. Ar jūsų darbe vykdomos kibernetinio saugumo pratybos? Jei taip, tai kaip dažnai?

Pažymėkite tik vieną.

- o Taip, bet rečiau nei kartą per metus.
- o Taip, 1 kartą per metus.
- o Taip, 2 kartus per metus.
- o Taip, 3 ir dažniau kartų per metus.
- o Pratybos mano darbe nevykdomos.

11. Ar Jūsų nuomone saugumo pratybos (*jei tokios buvo vykdomos*) davė rezultatų?

Pažymėkite tik vieną.

- o Taip, darbuotojai įgijo naujų žinių ir jas pradėjo taikyti praktikoje.
- o Ne, pratybos buvo neefektyvios.
- o Neturiu nuomonės.

- Pratybose nedalyvavau.

12. Ar galėtume keliais žodžiais ar sakiniais įvardinti kas, Jūsų nuomone, galėtų padėti sustiprinti kibernetinį saugumą Jūsų darbovietėje?

_____

_____