www.mruni.eu

Konstantin AGAFONOV

DAKTARO DISERTACIJA

KIBERNETINIO SAUGUMO VALDYMO MODELIS ELEKTRONINIAMS RINKIMAMS ĮGYVENDINTI

SOCIALINIAI MOKSLAI,
VADYBA (S 003)
VILNIUS, 2021

MYKOLO ROMERIO UNIVERSITETAS

MYKOLO ROMERIO UNIVERSITETAS

Konstantin Agafonov

KIBERNETINIO SAUGUMO VALDYMO MODELIS ELEKTRONINIAMS RINKIMAMS ĮGYVENDINTI

Daktaro disertacija
Socialiniai mokslai, vadyba (S 003)

Vilnius, 2021

Mokslo daktaro disertacija rengta 2015–2021 metais Mykolo Romerio universitete pagal Vytauto Didžiojo universitetui su Klaipėdos universitetu, Mykolo Romerio universitetu ir Šiaulių universitetu Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2019 m. vasario 22 d. įsakymu Nr. V-160 suteiktą doktorantūros teisę.

Mokslinis vadovas:
prof. dr. Tadas Limba (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, S 003).

TURINYS

SANTRUMPOS

angl. – sąvoka anglų kalba;
AOTD prie KAM – Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos;
CCDCOE – kibernetinės gynybos kompetencijų centras (angl. Cooperative Cyber Defence Centre of Excellence);
CEA – Kibernetinio saugumo stiprinimo aktas (angl. Cybersecurity Enhancement Act);
CERT – kompiuterių incidentų greito reagavimo komanda (angl. Computer emergency responce team, Computer Emergency Readiness Team);
CERT/CC – kompiuterių incidentų greito reagavimo komandos koordinavimo centras (angl. Computer Emergency Response Team Coordination Centre);
CIA – konfidencialumas, vientisumas, prieinamumas (angl. Confidentiality, Integrity, Availability);
CISSP – sertifikuotas informacinių sistemų saugos specialistas (angl. Certified Information Systems Security Professionals);
COBIT – informacijos ir susijusių technologijų kontrolės tikslai (angl. Control Objectives for Information and Related Technology);
COE – kompetencijų centras (angl. Center of Excellence);
DDoS – paskirstytas paslaugų atsisakymas (angl. Distributed Denial of Service);
DHS – Nacionalinio saugumo departamentas (angl. Department of Home Security);
DNS – domenų vardų sistema (angl. Domain Name System);
E&Y – Ernst and Young;
ENISA – Europos Sąjungos kibernetinio saugumo agentura (angl. European Union Agency for Cybersecurity);
ES – Europos Sąjunga;
GAO – Vyriausybės atskaitomybės tarnyba (angl. Government Accountability Office);
IEC – Tarptautinė elektrotechnikos komisija (angl. International Electrotechnical Commission);
IP – interneto protokolas (angl. Internet Protocol);
IRT – informacinės ir ryšių technologijos;
ISACA – Informacinių sistemų audito ir kontrolės asociacija (angl. Information Systems Audit and Control Association);
ISO – Tarptautinė standartizacijos organizacija (angl. International Organization for Standardization);
IT – informacinės technologijos;
ITU – Tarptautinė telekomunikacijų sąjunga (angl. International telecommunication union);
JAV – Jungtinės Amerikos Valstijos;
JT – Jungtinės Tautos;
liet. – sąvoka lietuvių kalba;

LR – Lietuvos Respublika;
LSD – Lietuvos Standartizacijos Departamentas;
NATO – Šiaurės Atlanto sutarties organizacija (angl. North Atlantic Treaty Organization);
NIST – Nacionalinis standartų ir technologijų institutas (angl. National Institute of Standards and Technology);
NKSC prie KAM – Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos;
NSW – Naujasis Pietų Velsas (angl. New South Wales);
SANS – SANS institutas (angl. SANS Institute);
ŠASO – Šiaurės Atlanto Sutarties Organizacija;
TEMPEST – elektromagnetinis įrenginių spinduliavimas;
TM – Teisingumo ministerija
UK – Jungtynė Karalystė (angl. United Kingdom);
US – Jungtynės Valstijos (angl. United States);
US GAO – Jungtinių Valstijų Vyriausybės atskaitomybės tarnyba (angl. United States Government Accountability Office);
USB – universali serijinė magistralė (angl. Universal Serial Bus);
VLE – Visuotinė lietuvių enciklopedija;
VRK – Vyriausioji rinkimų komisija;
VSD – Valstybės saugumo departamentas;
WISAC – Vandens informacijos mainų ir analizės centras (angl. Water Information Sharing and Analysis Center);
(ISC)² – Tarptautinis informacinių sistemų saugos sertifikavimo konsorciumas (angl. International Information System Security Certification Consortium).

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

PAGRINDINĖS SĄVOKOS

Elektroninis balsavimas – rinkimų procesas, kurio metu piliečiai dalyvaudami rinkimuose naudojasi bet kokiais elektroniniai įrenginiais, skirtais užfiksuoti jų pasirinkimą (pvz. elektroninės balsadėžės, kompiuteriai skirti balsuoti elektroniniu būdu rinkimų apylinkėje).

Elektroniniai rinkimai – balsavimo procesas, kurio metu savo pasirinkimo teisę įgyvendinantis asmuo naudojasi bet kokiomis šiuolaikinėmis ryšių ir informacinėmis technologijomis.

Internetinis balsavimas – rinkimų procesas, kurio metu piliečiai pareiškia savo nuomonę pasinaudodami balsavimo sistema veikiančia interneto technologijų pagrindu (pvz. Estijos internetinio balsavimo sistema).

Kibernetinė ataka – veiksmų seka, kuria objektą atakuojantys asmenys pasiekia tam tikrą tikslą (neteisėtą rezultatą) (Howard, Longstaff, 1998);

Kibernetinis incidentas – atakų grupė, kurią galima išskirti iš kitų atakų visumos, pasinaudojant būtent tai grupei būdingais požymiais: atakuojamųjų objektų savybės, atakų vykdymo metodas, siekiami tikslai, vieta ir laikas (Howard, Longstaff, 1998).

Kibernetinis saugumas – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2018).

Kibernetinio saugumo valdymas – būtini organizacijos veiksmai, nukreipti į vykdomos veiklos tęstinumo užtikrinimą ir galimos žalos organizacijos veiklai mažinimą, vykdant organizacijos informacinėms vertybėms ir kritinei infrastruktūrai grėsmę keliančių galimų saugumo incidentų prevenciją, taip pat jau įvykusių ar vykstančių kibernetinio saugumo incidentų poveikio minimizavimą.

ĮVADAS

Temos aktualumas. Šiuolaikinė visuomenė, jos gyvenimas ir socialiniai santykiai yra stipriai priklausomi nuo kibernetinės erdvės, todėl pasaulio informacinių technologijų specialistai ir įvairių mokslo krypčių atstovai deda dideles pastangas kibernetinio saugumo problemoms spręsti. Yra sukurtos ir plačiai taikomos informacijos saugumo valdymo technologijos, standartai, tačiau jie yra labiau susiję su informacijos saugumo ir technologijų valdymu organizacijos viduje, tuo tarpu kibernetinio saugumo valdymas apima ne tik vidinių grėsmių ir kibernetinio saugumo technologijų valdymą, bet ir galimų rizikų bei išorinių grėsmių stebėjimą, atsako į grėsmes galimybių bei grėsmių išvengimo priemonių vertinimą, personalo mokymą ir kibernetinio saugumo teisinį reguliavimą. Kompiuterinės sistemos ir technologiniai sprendimai, naudojami privataus sektoriaus veiklai organizuoti ir pertvarkyti, dabartiniais laikais plačiai pritaikomi ir viešajame sektoriuje. Valstybės ir piliečių nuolatinis bendravimas yra etapais perkeliamas į skaitmeninę erdvę. Toks perkėlimas sąlygoja greitesnį viešųjų paslaugų suteikimą piliečiams bei mažina viešojo administravimo institucijų veiklos krūvį. Technologinė revoliucija taip pat lemia bandymus naudoti šiuolaikines informacines ir telekomunikacines technologijas pasaulio valstybių politiniuose procesuose. Valstybės, naudodamos technologijas, bando priartinti piliečius prie šalies valdymo ir tiesioginio dalyvavimo įvairiuose šalyje vykstančiuose politiniuose procesuose, o vienas iš dažniausiai naudojamų politinio dalyvavimo ir gyventojų įtraukimo į politinius procesus įrankis yra elektroninis balsavimas.

Šiuolaikinis pasaulis pasiekė labai aukštą technologinį išsivystymo lygį, tačiau jis vis dar nėra saugus kibernetinio saugumo prasme: pastebimas tendencingas kibernetinių saugumo incidentų skaičiaus augimas, kibernetinių nusikaltėlių naudojamos įsibrovimų technologijos tampa sudėtingesnės ir vis sunkiau aptinkamos (Simmons ir kt., 2014), o tradiciniai technologiniai kibernetinio saugumo užtikrinimo įrankiai nėra pajėgūs atpažinti ir sustabdyti visas piktavalių rengiamas kibernetines atakas (Shabut ir kt., 2016). Yra atlikta nemažai mokslinių tyrimų, kurie yra susiję su informacijos saugumo valdymu organizacijose: informacijos saugumas nagrinėjamas atskirose mokslo srityse ne tik techniniu, bet ir vadybos, ekonomikos ir kitų mokslų kontekste (Ashenden, 2008; Bakshi ir kt., 2009; Jastiuginas, 2011; Johnson, 2015), tačiau to nepakanka, kad būtų galima sukurti kibernetinio saugumo valdymo modelį, kuris aiškiai ir vienareikšmiškai nusakytų kibernetinio saugumo valdymo aspektus, kuriant valstybės informacines sistemas ir teikiant elektronines paslaugas gyventojams. Nors ir nėra sukurtas bendras kibernetinio saugumo valdymo modelis, visos pasaulio valstybės supranta, kad yra būtina valdyti ir kruopščiai apsaugoti savo informacinius išteklius, o mokslininkai yra pažymėję, kad šalies ypatingos svarbos (kritinės) infrastruktūros saugumas yra būtinas ir turi būti valdomas kompleksiškai (Limba ir kt., 2017; NATO StratCom COE, 2018; Haynes, 2019; Giniotienė 2019; Sofiou, 2019).

Kibernetinio saugumo reiškinys yra nagrinėjamas nuo dvidešimtojo amžiaus paskutiniojo dešimtmečio. Pastebėtina, kad šios sąvokos esmė ir turinys kito nuo jos atsiradimo, o šis pasikeitimas yra siejamas su technologinių sistemų tobulėjimu ir

kaita. Kibernetinio saugumo (informacijos saugumo) reiškinys buvo pradėtas nagrinėti telekomunikacinių ir kompiuterinių sistemų apdorojamos informacijos saugumo kontekste, vėliau – kompiuterinėse sistemose perduodamos informacijos saugumo kontekste ir, galiausiai, informacijos vientisumo, prieinamumo, autentiškumo, patikimumo ir konfidencialumo užtikrinimo kontekstuose.

Viešojo sektoriaus atstovai, politikai, mokslininkai ir technologijų saugumo ekspertai sutaria, kad vien technologinių klausimų sprendimai nepanaikina visų problemų tol, kol nėra sukurtas kibernetinio saugumo valdymo modelis, taikytinas elektroniniams rinkimams įgyvendinti. Iš esmės problema slypi tame, kad kibernetinis saugumas turi būti traktuojamas ne tik kaip techninė disciplina ar pasiekiamas techninis lygis (Lowrie, 2015), bet kaip organizacijos valdymo koncepcija (Rainer ir kt., 2007). Koncepcija kurioje maksimaliai yra agreguojamos visos įmanomos priemonės: techninės, teisinės (Štitilis ir kt., 2017), o svarbiausia – vadybos strategijos ir pasiekiama tam tikra organizacijos branda (Lackram, Padayachee, 2018; Patiño, Yoo, 2018).

Kibernetinio saugumo valdymo problema elektroninių rinkimų įgyvendinimo kontekste pasaulyje yra mažai atskleista, bet aktuali. 2014 m. Jungtinės Tautos pradėjo pasaulinį kibernetinio saugumo stebėjimo projektą, kuris turėtų užtikrinti saugumo, žmogaus teisių stebėjimo bei ekonominių ir gerųjų valdymo praktikų įgyvendinimą. Šiuo disertaciniu darbu siekiama sukurti kibernetinio saugumo valdymo modelį, kuris gali būti pritaikytas, kuriant ir valdant kibernetinį saugumą elektroninių rinkimų sistemose. Elektroninių rinkimų įgyvendinimas yra vienas iš pagrindinių būdų skatinti piliečių dalyvavimą šalies politiniuose procesuose, o didžiausias šių sistemų trūkumas – sistemų saugumo stoka. Tikėtina, kad kibernetinio saugumo valdymo modelis, kuris bus kuriamas ir nagrinėjamas disertacijoje, pagreitins elektroninių rinkimų įgyvendinimą ir paspartins elektroninių rinkimų pripažinimą.

Temos ištirtumo lygis. Pasaulio mokslininkai, tarptautinės organizacijos ir kibernetinio saugumo technologinės ir programinės įrangos gamintojai kibernetinio saugumo valdymą nagrinėja įvairiais aspektais.

Mokslinėje literatūroje vis dar kyla diskusijos dėl paties kibernetinio saugumo reiškinio apibūdinimo. Kibernetinio saugumo reiškinį, jo kaitą ir esmę nagrinėjo Anderson, 2001; Ashenden, 2008; Jastiuginas, 2011; Agrawal, Campoe, Pierce, 2014; Alotaibi, Furnell, Clarke, 2016; Dykstra, 2017; Limba, Plėta, Agafonov, Damkus, 2017; Grincevičius, 2018 ir kiti pasaulio mokslininkai.

Autoriai Landwehr, Bull, McDermott, Choi, 1994; Howard, Longstaff, 1998; Weaver, Paxson, Staniford, Cullingham, 2003; Hansman, Hunt, 2003; Kjaerland, 2006; Gruschka, Jensen, 2010; Štitilis, 2011; Limba, Agafonov, 2012; Simmons, Shiva, Bedi, Dasgupta, 2014; Shabut, Lwin, Hossain, 2016 ir kiti mokslininkai rašo apie kibernetinio saugumo incidentų ir atakų klasifikavimo sistemas, identifikuoja galimus jų atlikimo būdus ir metodus.

Pasaulio mokslininkai taip pat nagrinėja kibernetinį saugumą teisiniais aspektais: Štitilis, 2013; Appazov, 2014; Lowrie, 2015; Deighton, 2015; Štitilis, Klišauskas, 2015; Kosseff, 2018, rizikos valdymo aspektais: Kroger, 2008; Ackermann, 2012; Agrawal, 2014; Chen, Pedrycz, Ma, Wang, 2014; Deighton, 2015; Proença, Estevens, Vieira, Bor-

binha, 2017; Vega, Arroyo, Yoo, 2017; Walker, 2018; Grincevičius, 2018; Patiño, Solís, Yoo, Arroyo, 2018, technologinio saugumo aspektais: Cayirci, Ghergherehchi, 2011; Solms, Niekerk, 2013; Donaldson, Siegel, Williams, Aslam, 2015; Alotaibi, Furnell, Clarke, 2016; Campbell, 2017; Collier, 2018, incidentų valdymo aspektais: Deighton, 2015; Beissel, 2016; Craig, Valeriano, 2016; Limba, Agafonov, 2012; procesų valdymo ir kontrolės aspektais: Rainer, Marshall, Knapp, Montgomery, 2007; Solms, 2009; Deighton, 2015; Latham & Watkins, 2016; Limba, Agafonov, Paukštė, Damkus, Plėta, 2017; Moschovitis, 2018; Patiño, Yoo, 2018, bei socialiniais ir kitais aspektais.

Kibernetinių incidentų atsiradimo ypatumus ir priežastis analizuoja Andersen, 2001; Barnes, Johnson, Nickelson, 2004; Masero, 2010; Wei, 2010; Cayirci, Ghergherehchi, 2011; Singer, Friedman, 2014; Craig, Valeriano, 2016; Voltz, 2016; Limba, Plėta, Agafonov, Damkus, 2017; Govindarasu, Hanas, 2017 ir kiti mokslininkai bei įvairios viešojo ir privataus sektoriaus organizacijos: ISO/IEC, 2013; USCERT, 2018; $(ISC)^2$, 2015; SANS, 2018 ir kt., kurios, siekdamos užtikrinti kibernetinio saugumo valdymą organizacijose, per pastaruosius du dešimtmečius sukūrė sistemas ir standartus, kurie gali būti naudojami, kuriant kibernetinį saugumą.

Elektronines rinkimų sistemas, jų veikimo principus, teorinius bei realius elektroninių balsavimo sistemų pažeidžiamumus ir jų atsiradimo priežastis nagrinėjo Jefferson, Rubin, Simons, Wagner, 2004; Kohno, Stubblefield, Rubin, Wallach, 2004; Filho, 2005; Fieldman, Halderman, Felten, 2006; Hursti, 2006; Gonggrijp, Hengeveld, 2007; Simmons, 2011; Limba, Agafonov, 2012; Chowdhury, 2013; Aranha, Karam, Miranda, Scarel, 2014; Brightwell, Cucurull, Galindo, Guasch, 2015; Karda, Kiraz, Bingöl, Birinci, 2016; Goldsmith, 2017; Halderman, 2017; Limba, Agafonov, Paukštė, Damkus, Plėta, 2017; Augoye, Tomlinson, 2018 ir kt., ypatingą dėmesį skirdami kibernetinių incidentų atsiradimo priežasčių nustatymui, taip siekdami identifikuoti esminius faktorius, darančius įtaką elektroninių rinkimų sistemų panaudojimui demokratiniuose procesuose.

Pažymėtina, kad, nors kibernetinis saugumas įvairiausiais aspektais yra pakankamai plačiai nagrinėjamas pasaulinėje mokslinėje literatūroje (taip pat ir elektroninių rinkimų saugumo užtikrinimo kontekste), vis dar nėra sukurtas kibernetinio saugumo valdymo modelis, kuris savyje sujungtų visapusišką požiūrį į kibernetinio saugumo grėsmes bei jų valdymo aspektus ir tokiu būdu suteiktų galimybę konstruoti maksimaliai saugias elektroninių rinkimų sistemas ir sėkmingai įgyvendinti elektroninius rinkimus.

Mokslinė problema: kokios yra kibernetinio saugumo sritys ir kaip turi būti organizuojamas kibernetinio saugumo valdymas, siekiant saugių ir patikimų elektroninių rinkimų įgyvendinimo?

Tyrimo objektas – elektroninių rinkimų įgyvendinimas kibernetinio saugumo valdymo kontekste.

Tyrimo tikslas – išanalizavus teorinio kibernetinio saugumo valdymo problematiką, sukurti kibernetinio saugumo valdymo modelį, kuris gali būti naudojamas įgyvendinant elektroninių rinkimų sistemas.

Siekiant tikslo, disertacijoje sprendžiami tokie **uždaviniai:**

1. Išanalizuoti kibernetinio saugumo valdymo teorinius aspektus, siekiant nustatyti pagrindines kibernetinio saugumo incidentų atsiradimo priežastis ir ypatumus, kibernetinio saugumo valdymo problematiką bei galimą kibernetinio saugumo incidentų įtaką elektroninių rinkimų sistemų kibernetiniam saugumui.
2. Išanalizuoti pasaulyje įvykdytas praktines ir teorines atakas prieš elektroninių rinkimų sistemas, siekiant nustatyti ir išryškinti labiausiai pažeidžiamus e-rinkimų sistemų elementus, bei pažeidžiamumus sąlygojusius aspektus.
3. Atsižvelgiant į teorinių kibernetinio saugumo valdymo aspektų analizės metu išryškėjusią kibernetinio saugumo valdymo problematiką, sukurti konceptualų kibernetinio saugumo valdymo modelį, taikytiną elektroninių rinkimų sistemų konstravimo, diegimo, valdymo ir naudojimo procesų metu, bei atlikti sukurto modelio vertinimui skirtą empirinį tyrimą.
4. Atsižvelgiant į empirinio tyrimo rezultatus, patikslinti konceptualų kibernetinio saugumo valdymo modelį, atlikti modelio struktūros, taikymo galimybių bei ribotumų analizę, pateikiant rekomendacijas, kaip modelis gali būti panaudojamas, įgyvendinant elektroninius rinkimus Lietuvoje.

Mokslinio tyrimo metodai. Disertacinis tyrimas yra suplanuotas trimis etapais. Pirmajame tyrimo etape, tiriant problema teoriniame lygmenyje, bus atliekama mokslinės literatūros ir kitų šaltinių analizė, palyginimas ir apibendrinimas, nagrinėjamos kibernetinių incidentų atsiradimo priežastis bei problematika. Antrajame disertacinio tyrimo etape bus formuojamas pradinis teorinis kibernetinio saugumo valdymo modelis elektroniniams rinkimams įgyvendinti, bei bus atliktas empirinis tyrimas (ekspertinis interviu). Siekiant išnagrinėti disertacinio darbo mokslinę problemą ekspertinio interviu metu bus apklausi ekspertai tiesiogiai dirbantys su kibernetinio saugumo valdymu ir įgyvendinimu, kibernetinio saugumo strategijos ir politikos formavimu bei technologiniu kibernetinio saugumo užtikrinimu. Trečiajame tyrimo etape, atsižvelgiant į empirinio tyrimo rezultatus, bus atliekamas teorinio kibernetinio saugumo valdymo modelio koregavimas, bei pateikiamą patikslinto kibernetinio saugumo valdymo modelio elektroniniams rinkimams įgyvendinti struktūros analizė. Tyrimo pabaigoje bus panaudojamas apibendrinimo metodas formuluojant teorinio ir empirinio tyrimų išvadas, taip pat pateikiamos rekomendacijos elektroninių rinkimų įgyvendinimui.

Disertacijos ginamieji teiginiai:

1. Kibernetinio saugumo valdymas dažniausiai suprantamas kaip technologinių priemonių taikymas organizacijos veiklos procesuose, tačiau tokia kibernetinio saugumo valdymo samprata yra labai ribojanti ir neapimanti visos organizacijos veiklos sričių: vadovavimo, teisinio reguliavimo, technologijų, rizikų ir incidentų valdymo, organizacijos saugumo kultūros.
2. Kibernetinio saugumo valdymo modelis, kuriame yra integruotos technologinės, teisinės, organizacinės bei fizinės saugos priemonės, gali būti naudojamas, kuriant saugią ir patikimą elektroninių rinkimų sistemą.
3. Sukurto kibernetinio saugumo valdymo modelio panaudojimas elektroninių rinkimų sistemų kūrimo ir diegimo procese suteikia galimybę labiau pasitikėti

sistemomis, kurios naudojamos rinkimams, bei gali paskatinti valstybių piliečius aktyviau dalyvauti politiniuose procesuose.

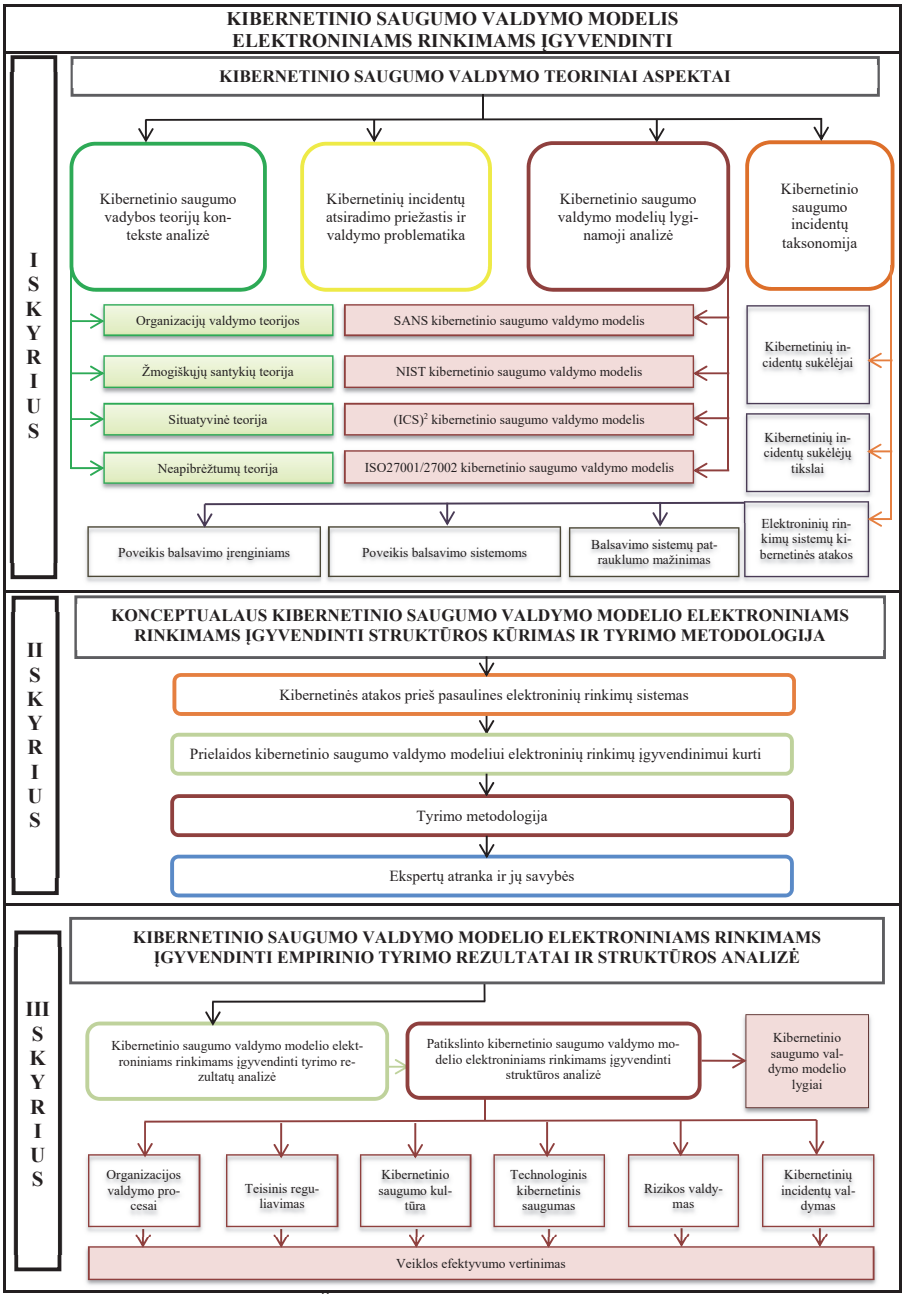
Darbo naujumas ir praktinis reikšmingumas. Pasaulyje kibernetinio saugumo reiškinys yra tiriamas įvairių mokslo šakų, dažniausiai – gamtos, technologijų ir socialinių sričių mokslininkų. Tačiau pažymėtina, kad mokslininkai nagrinėja kibernetinio saugumo valdymo problemą išskirtinai savo mokslo srities kontekste, nesigilindami į kitų mokslo šakų formuojamą problematiką. Taip sukuriama ydinga praktika, kai kibernetinis saugumas suprantamas ne kaip vientisas reiškinys, sujungiantis savyje visas mokslo sritis, bet kaip atskirų mokslo sričių tyrimo objektas. Atkreiptinas dėmesys, kad vien tik kompleksiškas požiūris į kibernetinio saugumo valdymą gali suteikti galimybę visapusiškai įvertinti kibernetinio saugumo spragas bei identifikuoti geriausius šių spragų pašalinimo būdus ir metodus. Šio disertacinio darbo naujumas ir reikšmingumas pasireiškia tuo, kad į kibernetinio saugumo valdymą žvelgiama per įvairių mokslo sričių prizmę, taip pat kad yra sukuriamas ir nagrinėjamas kibernetinio saugumo valdymo modelis, kurio įgyvendinimas gali užtikrinti elektroninių rinkimų sistemos sukūrimą Lietuvoje.

Atlikus mokslinės literatūros ir kitų šaltinių analizę disertacijos tema, buvo identifikuoti kibernetinio saugumo pažeidžiamumus sąlygojantys veiksniai, kibernetinių incidentų atsiradimo priežastys, sukurta kibernetinio saugumo incidentų taksonomija elektroninių rinkimų sistemų kontekste. Teorinių tyrimų metu taip pat buvo analizuojami pasaulio mokslininkų tyrimai, glaudžiai susiję su kibernetinio saugumo pažeidžiamumais šiuo metu veikiančiose ar anksčiau veikusiose elektroninių rinkimų sistemose. Vadovaujantis teorinių tyrimų metu sukauptais duomenimis, buvo sukurtas pradinis kibernetinio saugumo valdymo modelis, kuris gali būti naudojamas elektroninių rinkimų sistemų kibernetiniam saugumui užtikrinti, bei atliktas šio modelio empirinis tyrimas, suteikęs tyrėjui galimybę patikslinti pradinį kibernetinio saugumo valdymo modelį ir pritaikyti jį elektroninių rinkimų sistemoms įgyvendinti.

Disertacinis darbas identifikuoja bendrus šiuolaikinio kibernetinio saugumo valdymo probleminius aspektus organizacijose, taip pat pasiūlo šių problemų sprendimo metodus bei aiškiai apibrėžia kibernetinio saugumo valdymo modelį, kuris gali būti panaudojamas, kuriant ir diegiant elektroninių rinkimų sistemas. Disertaciniame darbe pateikiamas kibernetinio saugumo valdymo modelis taikytinas, siekiant užtikrinti sklandų kibernetinio saugumo valdymo procesą, kuriant ir įgyvendinant elektroninių rinkimų sistemas Lietuvoje, taip pat vykdant jų eksploatavimą. Tikėtina, kad, naudojant sukurtą, techniškai neutralų, kibernetinio saugumo valdymo modelį, elektroninių rinkimų sistemų įgyvendinimas ir naudojimas Lietuvoje greitu laiku taps realybe.

Disertacinio darbo struktūra. Disertacinį darbą sudaro trys dalys (žr. 1 paveikslą). *Pirmoje dalyje* yra nagrinėjami kibernetinio saugumo valdymo teoriniai aspektai: kibernetinis saugumas nagrinėjamas organizacijų valdymo, žmogiškųjų santykių, situatyvinės ir aplinkos neapibrėžtumo teorijų kontekstuose; analizuojami kibernetinio saugumo incidentų atsiradimo priežastys ir ypatumai; aptariama kibernetinio

saugumo valdymo problematika; aptariami ir palyginami kai kurie pasaulyje egzistuojantys kibernetinio saugumo valdymo modeliai ir jų panaudojimas organizacijos veiklos procesuose; aptariamas kibernetinio saugumo valdymas elektroninių rinkimų sistemų kūrimo ir diegimo kontekste; pateikiama kibernetinio saugumo taksonomija, aprašanti kibernetinio saugumo incidentų rūšis, incidentų sukėlėjus ir jų tikslus, kibernetinių nusikaltėlių taikomus kibernetinių atakų metodus; nagrinėjami elektroninių balsavimo sistemų pažeidžiamumai. *Antroje dalyje* pristatomas teorinių įžvalgų pagrindu sukurtas konceptualus kibernetinio saugumo valdymo modelis ir vykdyto empirinio tyrimo metodologija. *Trečioje dalyje* aprašomi kibernetinio saugumo valdymo modelio empirinio tyrimo rezultatai, pateikiama detali kibernetinio saugumo valdymo modelio struktūros analizė bei nagrinėjamas sukurto kibernetinio saugumo valdymo modelio pritaikomumas, įgyvendinant elektronines rinkimų sistemas Lietuvoje. *Darbo pabaigoje* yra pateikiamos išvados ir rekomendacijos.



Šaltinis: *parengta autoriaus*

1 paveikslas. *Disertacinio darbo struktūros loginė schema*

1. KIBERNETINIO SAUGUMO VALDYMO TEORINIAI ASPEKTAI

Galima teigti, kad dabartinėje visuomenėje, kurios egzistavimas ir kasdienė įprastinė veikla yra pagrista technologijomis, kibernetinis saugumas yra tapęs pačiu svarbiausiu visuomenės gyvavimo aspektu. Valdžios institucijos, finansų sektorius, viešąsias ir privačias paslaugas teikiančios organizacijos savo įprastoje kasdienėje veikloje naudoja informacines technologijas bei šių technologijų sukurtus produktus ir, be jokių abejonių, visos šios organizacijos yra stipriai priklausomos nuo kibernetinio saugumo (Bernier M., 2013; Limba ir kt., 2017; Prasad, Rohokale, 2020). Viešasis ir privatusis sektoriai kasmet sumoka milijonus eurų už technologijas ir produktus, skirtus jų veiklos saugumui užtikrinti: programinė ir techninė įranga yra nuolat atnaujinama, apsaugos sprendimai tobulėja, tačiau užtikrinti visišką arba bent jau priimtiną kibernetinį saugumą vis dar nėra įmanoma (Craig, Valeriano, 2016; Kovacich, 2016).

Pagrindinė susidariusios situacijos problema slypi tame, kad dažniausiai saugumas vis dar traktuojamas kaip technologinis aspektas ar technologija, kurią galima lengvai įgyvendinti organizacijos viduje, o šios įgyvendinimas užtikrins organizacijos kibernetinį saugumą (Dalziel, 2016). Šis požiūris dabartiniame pasaulyje turi būti pakeistas, nes šiuolaikinis kibernetinis saugumas yra ne tik technologinių aspektų rinkinys, bet reiškinys, kurį sudaro daug platesnis disciplinų sąrašas (Tisdale, 2015; Limba ir kt., 2017). Šioje disertacinio darbo dalyje bus nagrinėjami šiuolaikinio kibernetinio saugumo valdymo teoriniai aspektai; bus apžvelgiama kibernetinių atakų taksonomija; analizuojami atakų vektoriai bei kibernetinių atakų metodai, naudojami siekiant pažeisti organizacijos infrastruktūrą; taip pat bus nagrinėjamos dažniausiai pasitaikančios kibernetinio saugumo klaidos, kurios atsiranda organizacijų veikloje, siekiant apsisaugoti nuo pažeidžiamumų.

Kaip jau buvo pažymėta anksčiau, šiandieninis kibernetinis saugumas neturi būti suprantamas vien tik kaip technologinė disciplina. 2014 metais Lietuvos Respublikos Seimo priimtame Lietuvos Respublikos Kibernetinio saugumo įstatyme kibernetinis saugumas yra apibrėžiamas 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*. 2018 metų Lietuvos Respublikos Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatyme kibernetinio saugumo sąvoka yra pakeičiama ir kibernetinis saugumas yra suprantamas kaip *visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą*. Lyginant šiuose įstatymuose apibrėžtą kibernetinio saugumo sąvoką, galima pastebėti, kad 2018 metų Kibernetinio saugumo įstatymo pakeitimo įstatyme

kibernetinis saugumas pradedamas traktuoti ne kaip teisinių, informacijos sklaidos, organizacinių ir techninių priemonių panaudojimas, siekiant reaguoti į kibernetinius incidentus, bet kaip priemonių rinkinys, kurio panaudojimas nukreiptas į atsparumo kibernetiniams incidentams didinimą. Šių dviejų sąvokų skirtumas rodo kibernetinio saugumo supratimo evoliuciją, kadangi būtent atsparumo grėsmėms (veiksniams sąlygojantiems incidentų atsiradimą) didinimas ir užtikrinimas gali padėti sėkmingai priešintis ir valdyti kibernetinį saugumą.

Vadovaujantis įstatymu patvirtintais kibernetinio saugumo ir kibernetinio incidento apibrėžimais, galima nustatyti svarbiausius tikslus, siekiant užtikrinti kibernetinį saugumą:

- *autentiškumas,* kuris užtikrina, kad informacija, esanti tam tikruose informaciniuose ištekliuose (perduodama telekomunikacinėmis technologijomis), yra tikra ir nepakeista neteisėtos prieigos prie jos metu;
- *konfidencialumas*, kuris užtikrina, kad tik įgalioti asmenys galėtų gauti, keisti ar tvarkyti informaciją;
- *vientisumas*, kuris užtikrina, kad tik įgalioti asmenys ar procesai galėtų atlikti bet kokius sistemos pakeitimus;
- *prieinamumas*, užtikrinantis, kad tik įgalioti subjektai turės prieigą prie informacijos ar išteklių, kurie yra saugomi ar naudojami infrastruktūroje.

Pastebėtina, kad anksčiau minėti tikslai gali būti klaidingai tapatinami su informacijos saugumo tikslais (*angl. CIA triada: Confidentiality, Integrity, Availability*), tačiau pažymėtina, kad informacijos saugumo terminas dažniausiai vartojamas siauresniame kontekste ir dažniausiai taikomas vienos ribotos informacinės sistemos saugumui nusakyti, tuo tarpu kibernetinio saugumo terminas vartojamas organizacijos ar šalies kibernetinės erdvės kontekste ir apima ne tik konkrečios informacijos ar informacinės sistemos saugumą, bet ir visų ryšių ir informacinių technologijų, bei socialinių (žmogiškųjų) aspektų saugumą (CISA, 2009; ISO, 2012; Solms, Niekerk, 2013; Johansen, 2020; Kaspersky, 2020).

Pažymėtina, kad kibernetinio saugumo sąvokos ištakos yra siejamos su informacinių ir telekomunikacinių technologijų raida per paskutiniuosius tris dešimtmečius. Būtent tos raidos veikiamas informacinių technologijų saugumo apibrėžimas ir jo suvokimas pasauliniame kontekste suponuoja dabartinės skirtingų kibernetinio saugumo sąvokų visumos atsiradimą. Kompiuterių saugumo reiškinio virsmas į duomenų saugumą, vėliau – į informacijos saugumą ir kibernetinį saugumą sudarė prielaidas kibernetinio saugumo reiškinį tapatinti vien tik su technologinėmis priemonėmis, kurios yra naudojamos informacinių išteklių apsaugai nuo kibernetinių incidentų (Maurer, Morgus, 2014; CCDCOE, 2015; Vishik ir kt., 2016; Galinec ir kt., 2017; Mishra ir kt., 2019; Gupta ir kt., 2020).

Kibernetinio saugumo sąvokos įvairiose pasaulio šalyse analizė suteikia galimybę pastebėti, kad kibernetinis saugumas įvairiose pasaulio valstybėse yra apibrėžiamas ir suprantamas skirtingai. Tačiau dažniausiai jis yra tapatinamas su valstybių galimybėmis priešintis kibernetiniams incidentams (atstatyti kibernetinę erdvę po įvykusio incidento), kad šių incidentų atsiradimas arba jų sukelti padariniai kiek įmanoma

mažiau veiktų šalies kibernetinę erdvę (CCDCOE, 2015). Pasaulio mokslininkai savo tyrimuose taip pat pripažįsta, kad kibernetinis saugumas yra sąvoka, apimanti teisines, organizacines, technologines ir kitas priemones (Ten ir kt., 2010; Jastiuginas, 2011; Solms, Niekerk, 2013; Tisdale, 2015; Limba ir kt., 2017).

Šiuo metu kibernetinio saugumo supratimas visuomenėje pasiekė tam tikrą brandos lygį, o šio supratimo branda yra susijusi su greita informacinių ir telekomunikacinių technologijų plėtra į visas mūsų visuomenės gyvenimo sritis: tai ne tik platesnis interneto naudojimas visuomenėje ir joje vykstančiuose socialiniuose procesuose, bet ir verslo procesai bei efektyvesnis elektroninių viešųjų paslaugų teikimas (Limba ir kt., 2016). Pastebėtina, kad informacinių ir telekomunikacinių technologijų plėtra turi ir tam tikrą neigiamą poveikį: didėjant technologijų plėtrai, didėja ir šių technologijų sukuriamų grėsmių (pažeidžiamumo) lygis. Numanoma, kad pagrindinė didėjančio pažeidžiamumo problema gali būti susijusi su įvairiausiomis informacinėmis sistemomis bei šių sistemų tarpusavio integracijos proceso sudėtingumu: mažųjų informacinių sistemų elementai yra sujungiami arba integruojami į didesnes informacines sistemas, o dėl šių sujungimų padidėja sistemų sudėtingumas bei sukuriamos sąlygos pažeidžiamumams atsirasti ne tik sistemose, kurias naudoja skirtingos organizacijos, bet ir informacinėse sistemose, kurios naudojamos valstybės mastu. Šiuolaikinių technologijų panaudojimas dažniausiai yra susijęs su veiksmingumo didinimo poreikiu, tačiau dėl kibernetinio saugumo supratimo ribotumo ir ypač realios kibernetinės saugumo situacijos suvokimo trūksta tinkamo supratimo apie kylančias grėsmes ir šių grėsmių galimą įtaką visuomenei ar tam tikrai visuomenės daliai (Kroger, 2008; Cohen, 2015; Vidiveloo ir kt., 2016; Limba ir kt., 2017). Galima teigti, kad situacija su grėsmių kibernetiniam saugumui supratimu nėra visiškai beviltiška. Pasaulio šalys ir mokslininkai sutaria, kad, siekiant apsaugoti kritinę šalies infrastruktūrą (pvz., bankines sistemas, kritinę energetinę infrastruktūrą, elektroninių balsavimų sistemas ir kt.), yra būtinas kibernetinio saugumo valdymo modelis. *Ypatingos svarbos (kritinė) infrastruktūra* šio disertacinio darbo kontekste yra traktuojama kaip valstybės, organizacijos ar įmonės materialus ar nematerialus informacinis resursas, kurio neveikimas ar veiklos sutrikdymas gali padaryti didelės žalos nacionaliniam saugumui, šalies ūkiui, valstybės, organizacijos ar visuomenės interesams. Jau 2000 metais Jungtinės Amerikos Valstijos pažymėjo (vėliau jas palaikė ir kitos pasaulio šalys ir organizacijos), kad kibernetinis saugumas turi būti valdomas visapusiškai, o ne atskirose valstybės informacinėse sistemose (JAV GAO, 2007; Council of Europe, 2008; NATO, 2010; Lietuvos nacionalinė saugumo strategija, 2012; Johnson, 2015).

1.1. Kibernetinio saugumo kai kurių vadybos teorijų kontekste analizė

Kaip jau buvo kalbėta anksčiau, kibernetinis saugumas šiuo metu tampa prioritetiniu klausimu visose gyvenimo sferose. Kiekvienas visuomenės žingsnis, kiekvienas veiksmas daugiau ar mažiau yra siejamas su kibernetiniu saugumu. Visos šiuolaikinės visuomenės veiklos sferos yra grindžiamos technologijų panaudojimu: pradedant mobiliojo telefono ar viešojo transporto bilietų sistemų funkcionavimu ir baigiant valstybės gyventojams teikiamų viešųjų paslaugų administravimo sistemų veikimu.

Tokios veiklos kaip: elektros ir vandens tiekimas gyventojams, gatvių apšvietimo ir šviesoforų sistemos valdymas, pagalbos skambučių bendram pagalbos centrui apdorojimas yra nesuvokiami be technologijų, o technologijos kartu su savo teikiamais privalumais atsineša ir tam tikras grėsmes (Johnson, 2015). Būtent technologinis pasaulio išsivystymas, kuris stipriai pažengė į priekį per paskutiniuosius dvidešimt penkerius metus, ir atnešė mums kibernetines grėsmes, kurios kelia ypatingą riziką dabartiniam pasauliui (Loukas ir kt., 2013; Simmons ir kt., 2014).

Kibernetinio saugumo valdymas yra ne atskirų organizacijų individuali veikla, o šalies mastu vykdomas procesas. Valstybę šiuo atveju galima laikyti viena didele ir sudėtinga organizacija, kurios veikla yra vykdoma per tam tikras funkcinių sričių organizacijas, kurios yra daug smulkesnės ir atsako už tam tikras veiklas bei darbų tęstinumą. Dažnai valstybės nesusirūpina kibernetiniu saugumu tol, kol realybėje nepajaučia kibernetinių grėsmių poveikio sau ir savo valdomoms technologinėms sistemoms (ištekliams). Kai kibernetiniai išpuoliai ima kenkti valstybės įvaizdžiui, kibernetinio saugumo valdymo veikla tampa prioritetinė ir reikalaujanti ypač daug lėšų bei koordinavimo (Johnson, 2015).

Nagrinėjant kibernetinio saugumo valdymą vadybos teorijų kontekste, galima teigti, kad egzistuoja keletas kibernetinio saugumo valdymo dimensijų. Pirmoji dimensija gali būti siejama su organizacijos struktūra. Šis kontekstas leidžia valstybę, siekiančią užtikrinti kibernetinio saugumo valdymą, nagrinėti kaip organizaciją, kurios pagrindinis tikslas yra užtikrinti kibernetinį saugumą savo vidinėje ir išorinėje aplinkoje, sukurti „produktą“, kuris sąlygoja valstybės gerovę, kokybišką valstybės technologinės infrastruktūros valdymą ir paslaugų teikimą valstybės nariams. Nagrinėjant šią dimensiją, šiame disertaciniame darbe bus taikomos H. Fajolio ir M. Vėberio teorijos.

H. Fajolis savo moksliniuose darbuose tyrė galimybes didinti organizacijos veiklos efektyvumą per organizacijos vadovybės taikomus vadybos metodus, kuriuos jis laikė pagrindiniais katalizatoriais, skatinančiais organizacijos veiklos efektyvumo padidėjimą. Būtent H. Fajolis tvirtino, kad tinkami ir laiku panaudoti vadybos metodai yra ne kas kita, kaip žingsnis link organizacijos veiklos efektyvumo didinimo (Fajolis, 2005).

Savo knygos „Bendrasis ir pramonės valdymas“ įžangoje H. Fajolis tvirtina, kad valdymas yra be galo svarbus bet kuriai bendrovei, didelei ar mažai, ir jis gali būti naudojamas visose gyvenimo sferose: politikoje, prekyboje, religijoje ar bet kur kitur, o administracinė doktrina, sudaryta iš principų, taisyklių ir metodų rinkinių, siekia palengvinti valdymą visų tipų organizacijose (Šeldreik, 2001; Kostenko, Michalkina, 2014). Toks požiūris į valdymą taip pat gali būti taikomas ir kibernetiniam saugumui, kuris neabejotinai yra svarbus kiekvienai organizacijai (Soomro ir kt., 2016; Furnell ir kt., 2017; Haqaf, Koyuncu, 2018; Ursillo, Arnold, 2019).

Valdymą H. Fajolis apibrėžia kaip organizacijos ar įmonės vedimą į tikslą, siekiant optimalios naudos iš visų turimų išteklių ir sklandaus esminių funkcijų darbo (Fajolis, 2005). H. Fajolio doktrinoje yra išskiriamos šešios esminės funkcinės organizacijos veiklos sritys: techninė, komercinė, finansinė, apsauginė, buhalterinė ir administracinė veikla. Pažymėtina, kad šių funkcinių veiklų aktualumas egzistuoja ir šiais laikais (Makura, 2015; Haqaf, Koyuncu, 2018; Ursillo, Arnold, 2019).

Kibernetinio saugumo valdymas valstybėje taip pat gali, o gal net ir turi būti organizuojamas, vadovaujantis H. Fajolio doktrina. Fajolis savo darbuose ypatingą dėmesį skyrė valdymui ir administravimui, pabrėždamas, kad tai yra svarbiausia sritis, o šios veiklos vykdymas turi būti atliekamas pagal tam tikrą planą, o chaosas šioje veikloje yra visiškai neleidžiamas ir negalimas. Funkcinės srities valdymo planas turi būti sudarytas iš penkių etapų: siekiamų rezultatų numatymo; konkrečių veiksmų plano parengimo; komandos sudarymo ir funkcijų atskiriems komandos nariams numatymo; numatytų tikslų plano realizavimo ir veiksmų, reikalingų tikslams pasiekti, įgyvendinimo; plano vykdymo kontrolės, leidžiančios stebėti ir reaguoti į pasiektus rezultatus (Fajolis, 2005). Šie principai taip pat yra taikomi ir kibernetinio saugumo valdymo procese (Makura, 2015; Ursillo, Arnold, 2019).

H. Fajolis padarė išvadą, kad kiekvienas žinių ir kompetencijų rinkinys priklauso nuo faktiškai atliekamos esminės funkcijos ir darbuotojo „reikšmingumo" organizacijoje. Pasak H. Fajolio, geras vadovas turi būti pirmiausia geras administratorius, sugebantis numatyti, pasirengti, organizuoti, koordinuoti ir kontroliuoti. Pažymėtina, kad nagrinėjant kibernetinio saugumo valdymo organizacijoje aspektus pasaulio mokslininkai taip pat pateikia nuomonę, apie skirtingų profesinių gebėjimų ir valdymo įgūdžių būtinumą skirtingo lygio specialistams (Gleghorn, Gordon, 2012; Abuzaid, 2015; Haqaf, Koyuncu, 2018).

H. Fajolis pažymi, kad, norėdamas pasiekti organizacijos veiklos efektyvumą, įmonės personalas turi sugebėti sėkmingai vykdyti visas šešias esmines funkcijas, o administravimo funkciją išskyrė kaip vienintelę funkciją, kurios veikimas yra visų kitų funkcijų sudedamoji dalis (Urwick, 1934).

H. Fajolis suformulavo keturiolika integruoto administravimo principų (Bedeian, Wren, 2009), kurie yra aktualūs ir šiomis dienomis. Pažymėtina, kad Fajolio suformuluoti integruoto administravimo principai yra pagrindinių veiksnių, lemiančių valdymo efektyvumą, sąrašas, kurio pritaikymas organizacijos veiklos procesuose, anot H. Fajolio, yra būtinas, norint pasiekti vadovavimo veiksmingumą, neatsižvelgiant į tai, kokio organizacija yra didžio ir kokia yra organizacijos vidinė struktūra (Fajolis, 2005; Makura, 2015).

Kibernetinio saugumo valdymas taip pat gali būti nagrinėjamas šių principų kontekste, bet būtina pažymėti, kad, nagrinėjant kibernetinio saugumo valdymą valstybės mastu, t. y. traktuojant valstybę kaip organizaciją, vadovo funkcijas organizacijoje gali atlikti tik viena konkreti institucija, kurios atsakomybei yra priskiriama kibernetinio saugumo valdymo funkcija. Lietuvoje ši funkcija yra deleguota Nacionaliniam kibernetinio saugumo valdymo centrui, kuris pagal savo kompetenciją drauge su valstybės įstaigomis ir organizacijomis bei kitais ūkio subjektais sprendžia valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros kibernetinio saugumo klausimus. Kitos viešojo ir privataus sektorių organizacijos šiuo atveju gali būti traktuojamos kaip darbuotojai, kurie yra pavaldūs vadovui, bet, veikdamos kartu, siekia bendro tikslo – sklandaus valdymo šalies kibernetinio saugumo srityje.

Pažymėtina, kad visos organizacijos veiklos efektyvumas priklauso ne tik nuo to, kaip organizacijoje yra realizuojami administravimo principai, bet ir nuo to, kas

vadovauja pačiai organizacijai. H. Fajolio įsitikinimu, vadovas turi būti žmogus, kurio kvalifikacija yra grindžiama ekonomikos, technikos ir valdymo žiniomis, o pagrindinis vadovo darbas organizacijoje yra planų parengimas bei veiklos organizavimas. Sugretinant H. Fajolio teoriją ir kibernetinio saugumo valdymo problemą, galima daryti išvadą, kad vien tik technologijų išmanymas ir žinojimas nėra sėkmingo kibernetinio saugumo valdymo įgyvendinimo garantas. Organizacijos veiklos valdymas ir vadyba yra ta priemonė, kuri kuria kibernetinį saugumą (Soomro ir kt., 2016), o technologijos yra tik įrankis, kuris gali padėti pasiekti tam tikrus numatytus tikslus (Ursillo, Arnold, 2019). Technologijos kibernetinio saugumo valdymo kontekste yra tarsi kastuvas žemkasiui: be kastuvo duobės neiškasi, bet, jei nežinosi, kur tą duobę kasti ir kaip, tai ir kastuvas jokios naudos neduos.

M. Vėberio biurokratijos teorijos kontekste kibernetinio saugumo valdymas gali būti traktuojamas kaip tam tikrų valstybės veiklos funkcijų užtikrinimas, siekiant, kad visos už kibernetinį saugumą atsakingos institucijos ir organizacijos veiktų kaip viena labai gerai suderinta mašina.

M. Vėberio idealios biurokratijos modelis yra grindžiamas racionalios valdžios tipu, o pats modelis yra realizuojamas per biurokratinį administracinį personalą (Urbanovič, Smalskys, 2015; Serpa, Ferreira, 2019). M. Vėberis savo biurokratijos teorijoje suformulavo principus, kurie yra būdingi racionaliai biurokratinei organizacijai (Gerth, Mills, 1958), tačiau būtina pažymėti, kad tai nereiškia, kad biurokratijos modelis gali būti diegiamas tik viešojo valdymo struktūrose, kadangi modelio nuostatos kuo puikiausiai tinka ir privataus verslo organizacijoms (Brenner, 2013; Serpa, Ferreira, 2019), bet jo naudojimas turi tam tikrų išlygų, kadangi modelis yra gana statiškas, o šiuolaikiniame pasaulyje statinės (mechanistinės) organizacijos turi tam tikrus trūkumus ir negali taip greitai reaguoti į aplinkos pokyčius (Burns, Stalker, 1961), kaip tai daro organinės organizacijos.

Visi Vėberio modelio principai taip pat yra taikomi ir šiuolaikinių informacijos apsaugos ir kibernetinio saugumo valdymo sistemose (Frangopoulos ir kt., 2008). Principų panaudojimas kuriant kibernetinį saugumą organizacijoje gali padėti labai tiksliai apibrėžti vidinius procesus, kurie vyksta tarpinstitucinio bendradarbiavimo lygyje (Brenner, 2013, Yoe ir kt., 2015; Serpa, Ferreira, 2019). Laikantis M. Vėberio suformuluotų principų, galima sukurti stiprią kibernetinio saugumo valdymo „koaliciją“, kurios nariais taptų telekomunikacinių paslaugų tiekėjai, ryšių reguliavimo institucijos, akademinė bendruomenė, viešojo valdymo sektoriaus atstovai ir privačios bendrovės.

Žinoma gali atsirasti šios idėjos įgyvendinimo priešininkų, kurie sakys, kad kibernetinis saugumas negali būti konstruojamas pagal M. Vėberio siūlomą modelį. Pagrindiniai tokių priešininkų argumentai yra grindžiami įsitikinimais, kad:

- statiški modeliai yra netinkami kibernetinio saugumo užtikrinimui, kadangi jie yra nelankstūs, o kibernetinės erdvės grėsmių diapazonas nuolat plečiasi milžinišku greičiu. Dėl šios priežasties kibernetinio saugumo valdymo modelis turi būti dinamiškas bei sugebantis greitai reaguoti į aplinkos pokyčius (Blasch ir kt., 2014; Sheymov, 2016; Singh, 2018; Petuchov, Gusnin, 2019);

- kibernetinis saugumas yra labai dinamiška veikla, kurios negalima sunormuoti standartiniais atvejais, kadangi kibernetiniai pažeidėjai yra labai išradingi ir kūrybingi žmonės, sugalvojantys vis naujų ir iki šiol nežinotų atakų ir saugumo spragų išnaudojimo būdų, kurie per du dešimtmečius evoliucionavo nuo virusų, kurie tiesiog lėtindavo kompiuterių veikimą arba kitokiais būdais lėtindavo informacinių sistemų darbą, iki piktybinės (*angl. malware*) programinės įrangos, kuri, maskuodamasi kompiuterinėse sistemose, tiesiog vagia duomenis ir persiunčia į kibernetinių nusikaltėlių rankas (Singh, 2017; Minchev, 2018; DNR Digital, 2020; Mukherjee, 2020).

Šie argumentai, žinoma, yra labai svarūs, bet galima prieštarauti jiems, numatant vieną svarbų dalyką: H. Fajolio ir M. Vėberio organizacijų modelių tarpusavio sinteze.

Kitais žodžiais tariant, M. Vėberio modelis gali būti esminiu organizacijos formavimo modeliu, kuris nustatytų aiškius organizacijos veikimo principus ir instrukcijas, kuriomis vadovaujasi visos organizacijos nariai, vykdydami savo kasdienę veiklą (Serpa, Ferreira, 2019). Kadangi kibernetinio saugumo užtikrinimas nagrinėjamas valstybiniu lygiu, tai šiuo atveju visa valstybė yra traktuojama kaip organizacija, o tiksliau – visos privataus verslo ir viešojo valdymo organizacijos, kurios vienaip ar kitaip yra susijusios su kibernetinio saugumo užtikrinimu valstybėje.

Šiame modelyje gali būti aprašytos valstybinių institucijų bendradarbiavimo ir veiklos taisyklės, numatyti pavaldumo ir atskaitomybės ryšiai, nurodytos standartinės veiklos ir šių veiklų užtikrinimo sąlygos ir kt. Kibernetinio saugumo valdymas būtų grindžiamas tiksliomis nuorodomis į tai, kaip turi būti organizuojamas kibernetinių incidentų stebėjimas, reagavimas į šios incidentus, numatyti veiksmai, kurių privalo imtis organizacijos, atlikdamos savo kasdienius darbus.

Faktiškai visas organizacijos veiklos procesas gali būti grindžiamas M. Vėberio modeliu, tačiau aiškiai suprantama, kad dėl besikeičiančios kibernetinio saugumo situacijos pasaulyje tas statiškas modelis ne visuomet gali būti taikomas realybėje. Atsiranda naujos grėsmės, nauji nusikaltimų ir atakų tipai ir metodai, o jie kaip tik ir kels naująsias grėsmes visai organizacijai.

Būtent šioje vietoje reikia atsigręžti į H. Fajolį ir į jo pasiūlytą modelį, kuriame vadovui yra skiriamas didžiausias vaidmuo, vykdant planavimą, kuris taip pat turi būti susietas su nenumatytomis situacijomis, kurių kibernetiniame saugume, be jokių abejonių, yra, buvo ir bus.

H. Fajolis savo modelyje numatė tam tikrus principus (komandų vienovės, valdžios, disciplinos, hierarchijos, tvarkos, iniciatyvos, komandinės dvasios), kuriuos galima būtų taikyti bendrame jo ir M. Vėberio modelių sintezės kontekste, t. y. sujungti statišką ir nelankstų M. Vėberio modelį su dinamiškesniu H. Fajolio modeliu. Toks sujungimas leistų vienu metu taikyti ir griežto instrukcijomis grįsto valdymo ir funkcijų vykdymo modelį su situaciniu valdymu tuomet, kai aplinka paveikia organizaciją ir organizacijai būtina bei gyvybiškai svarbu staigiai reaguoti į išorinius aplinkos pokyčius. Šių dviejų valdymo modelių taikymas leistų organizacijai tapti lankstesnei, ir tokiu būdu būtų galima užtikrinti didesnį organizacijos atitikimą ją supančiam pasauliui.

Kaip buvo minima anksčiau, kibernetinio saugumo valdymas valstybėje šioje disertacijoje yra nagrinėjamas per globalizavimo prizmę, t. y. valstybė yra traktuojama

kaip organizacija, o valstybės institucijos ar privataus verslo įmonės – kaip tos organizacijos nariai. Viešojo ir privataus sektoriaus bendradarbiavimas kibernetinio saugumo srityje šiais laikais tampa vis aktualesnis (ESCO, 2016; Spencer, 2017; ENISA, 2018; Bossong, Wagner, 2018; Bayern, 2019; Kosseff, 2020; Lardy, 2020). Vadovaujantis minėtu požiūriu, galima teigti, kad anksčiau minėti H. Fajolio ir M. Vėberio modeliai yra tinkami globalaus valdymo organizavimo situacijoje, kai bendravimas tarp organizacijos narių yra vykdomas, pasitelkiant aiškiai struktūrizuotus hierarchinius modelius (McNamara, 2009; Serpa, Ferreira, 2019). Tačiau nereikia pamiršti, kad prieš tai nagrinėti organizacijos nariai yra ne pavieniai asmenys, o didelės lokalios organizacijos (institucijos), kurios savo ruožtu yra sudarytos iš tam tikrų struktūrinių padalinių (pavienių narių), vykdančių aiškiai nurodytas funkcijas. Galima būtų teigti, kad kibernetinio saugumo valdymą šiose organizacijose galima būtų nagrinėti pagal H. Fajolio ir M. Vėberio teorijas, bet tai nėra visiškai teisingas požiūris. Klasikinės teorijos kontekstas, naudotas organizacijos struktūros dimensijoje, nusako ir tam tikrus šių teorijų aspektus, kurie yra aktualūs organizacijos narių tarpusavio santykiams, bet šie santykiai klasikinėje organizacijos teorijoje buvo nagrinėjami labai skurdžiai. Dėl šios priežasties kibernetinio saugumo valdymą yra būtina nagrinėti žmogiškųjų santykių teorijos kontekste.

Reikia pažymėti, kad optimalus darbo pasidalinimas, darbų nuasmeninimas ir aiškios instrukcijos darbuotojams yra labai geras ir be jokių abejonių svarbus dalykas, bet, valdant organizacijas, reikia galvoti ne tik apie standartų ir taisyklių taikymą ir universalistinį požiūrį į valdymą, bet ir atsižvelgti į tam tikrus darbuotojų tarpusavio santykius ir partikuliaristinį požiūrį organizacijoje (Hampden-Turner, Trompenaars, 2011; Tisdale, 2015).

Klasikinėje organizacijų valdymo teorijoje buvo nagrinėjami organizacijos modeliai bei vyravo požiūris į žmogų kaip į darbo įrankį, buvo numatomas griežtas darbų reglamentavimas ir deklaruojama, kad aukštas atlygis už darbą gali išspręsti darbo našumo problemą ir paskatinti organizacijos narius didinti organizacijos efektyvumą (Serpa, Ferreira, 2019). Laikui bėgant, paaiškėjo, kad klasikinės organizacinės teorijos požiūris nėra visiškai tikslus, o tai savo ruožtu paskatino žmogiškųjų santykių teorijos atsiradimą (Zakarevičius, 2002). Didžiausias dėmesys šioje teorijoje yra skiriamas organizacijų narių tarpusavio santykiams, bendradarbiavimo aspektams, žmogaus socialinių poreikių tenkinimo ir elgesio organizacijoje klausimams, o jų svarbą E. Majo grindė atlikto Hotorno eksperimento išvadomis. Žmogiškųjų santykių teorijoje taip pat yra aptariami ir dabartiniais laikais aktualus klausimai – darbo našumo priklausomybė nuo socialinių aplinkybių, susidariusių organizacijoje, bei nuo organizacijos narių tarpusavio santykių, taip pat nuo santykių tarp organizacijos vadovybės ir organizacijos narių. Visi šie aspektai yra aktualūs ir kibernetinio saugumo kontekste (Hui ir kt., 2010; Evans ir kt., 2016; Kaspar, Shears, 2017; Limba ir kt., 2017; Houston, 2019; Petryni, 2019; Garcia, 2020; Lahcen ir kt., 2020).

Nagrinėjant kibernetinį saugumą per žmogiškųjų santykių teorijos požiūrio prizmę, galima būtų drąsiai tvirtinti, kad organizacijoje, siekiant užtikrinti kibernetinę saugą, turi būti puoselėjamas būtent partikuliaristinis požiūris.

Kibernetinio saugumo valdymas iš esmės yra apibrėžiamas kaip techninių, administracinių ir kitų priemonių panaudojimas, stebint, reaguojant ar vengiant saugumo incidentų, o, užtikrinant kibernetinį saugumą, būtina vadovautis teisiniais aspektais ir konkrečiomis techninėmis instrukcijomis, kadangi tik šių instrukcijų vykdymas gali nurodyti tinkamus ir apgalvotus veiksmus, užtikrinant saugumą. Galima teigti, kad valdymas šioje situacijoje turi būti aiškiai reglamentuotas ir vykdomas pagal klasikinės teorijos postulatus, bet tuo pačiu neturi būti pamirštos žmogiškųjų santykių teorijos: darbuotojai turi būti valdomi ir turi paklusti vadovui, kuris, savo ruožtu, savo valdymą grįstų ne tik asmenine nuomone ar patirtimi, bet ir gebėtų išklausyti savo pavaldinių idėjas, pastebėjimus ir pasiūlymus, sugebėtų tinkamai motyvuoti savo darbuotojus, kaip tai siūlė daryti Frederickas Irvingas Herzbergas savo motyvavimo teorijoje (Mescon ir kt., 1985), bei vadovautis Mary Parker Follett siūlytu efektyviu grupinės veiklos gerinimo receptu, kurį įmanoma įgyvendinti tik tuomet, kai vadovas ir pavaldiniai dirba išvien ir savo darbe vadovaujasi principu „vienas su kitu“, o ne „vienas virš kito“ (Mele, Rosanas, 2003; Kessler, 2013).

Kibernetinio saugumo valdymas nagrinėjamas per žmogiškųjų santykių teorijos prizmę gali pasirodyti keistokas, bet, vadovaujantis šios teorijos postulatais, galima būtų paaiškinti naudojamų kibernetinio saugumo valdymo mechanizmų sėkmingumą. Geri santykiai kolektyve bei kolektyvinis mąstymas organizacijos viduje, nuomonių aptarimai ir idėjų pasidalinimas gali paskatinti darbuotojus teikti naujus kibernetinio saugumo techninio aptikimo priemonių panaudojimo idėjas. Būtent bendradarbiavimas ir dalinimasis patirtimi, o ne aklas instrukcijų vykdymas padeda sukurti naujus saugumo mechanizmus ir atremti kibernetines atakas (Oltsik, 2016; Hadlington, 2017; Gosgrove, 2019; Zorz, 2020).

Lietuvoje institucijos, bendradarbiaudamos kibernetinio saugumo srityje, nesiekia kažkokių „asmeninių“ interesų ar galios užtikrinimo tam tikroje sferoje. Privataus verslo bendrovės bando bendradarbiauti su valstybiniu sektoriumi, ir tas bendradarbiavimas nėra grindžiamas teisiniais įpareigojimais (įstatymais ir nutarimais). Bendradarbiavimo varomoji jėga iš esmės yra noras sukurti saugią ir patikimą kibernetinę erdvę, kurioje ir valstybės institucijos, ir privačios bendrovės, ryšio paslaugų tiekėjai ir vartotojai jaustųsi saugiai. Šioje situacijoje aiškiai matomas kolektyvinis noras kurti kibernetinį saugumą bendromis jėgomis, o šios pastangos yra ne kas kita, kaip žmogiškųjų santykių teorijos pamatinės nuostatos, kurios gali būti taikomos ne tik organizacijų viduje, bet ir organizacijoms, kurios dalyvauja valstybės kibernetinio saugumo užtikrinimo procese.

Galima sakyti, kad kibernetinio saugumo valdymas santykių dimensijoje turi būti nagrinėjamas per klasikinės ir žmogiškųjų santykių teorijos simbiozės prizmę, pasirenkant ir aiškiai apibrėžiant, kokiomis aplinkybėmis vadovautis klasikų ar žmogiškųjų santykių teorijos atstovų nuomonėmis.

Praeito amžiaus septinto ir aštunto dešimtmečių sandūroje atsirado situatyvinė teorija. Šios teorijos šalininkai teigė, kad organizacijose dažnai pasitaiko analogiškos, jau prieš tai susidariusios konkrečios situacijos, todėl tokioms situacijoms spręsti gali būti parengiamos instrukcijos ir sprendimo metodai, kurie jau buvo aprobuoti anksčiau ir

kuriuos, tikėtina, bus galima panaudoti vėl. Tokiu būdu organizacijos gali spręsti tipines problemas, taip gerindamos savo veiklos efektyvumą (Kessler, 2013; Zhao, 2020).

Situatyvinė teorija gali būti taikoma, nagrinėjant kibernetinio saugumo problemą konkrečios organizacijos nario (institucijos), kuris vykdo konkrečią kibernetinio saugumo valdymo funkciją, dimensijoje. Kitaip galima pavadinti šią dimensiją aplinkos poveikio dimensija.

Kibernetinio saugumo valdymo kontekste situatyvinės teorijos panaudojimas gali būti naudingas, sprendžiant tam tikrus saugumo incidentus, kai tokie saugumo incidentai jau yra nutikę praeityje ir jų scenarijai kartojasi (Ferdinand, Benham, 2017; Harry, 2018, Chase, 2019; Zhao, 2020). Praktikoje, užtikrinant kibernetinį saugumą, labai dažnai yra vadovaujamasi situatyvinės teorijos nuostatomis, kuomet tam tikri saugumo pažeidžiamumai, jau kažkada nutikę organizacijoje, yra suklasifikuojami į tam tikras grupes, kurios yra vienalytės pagal savo požymius ar veikimo metodus. Vėliau yra aprašomos standartinės veiklos procedūros, kurios yra vykdomos, siekiant suvaldyti incidentą ir neleisti jam plisti, parengiami reagavimo į kibernetinius incidentus planai ir instrukcijos (Miller, 2019; Radar First, 2020). Dauguma technologinių sprendimų, naudojamų kibernetinėms grėsmėms aptikti ir valdyti (įsibrovimų aptikimo sistemos, tinklų veiklos sutrikimų sistemos ir sensoriai, antivirusinės programos ir kt.), veikia panaudodamos tokius instrukcijų rinkinius, kurie yra kuriami, atsižvelgiant į jau aptiktus saugumo pažeidžiamumus.

Pažymėtina, kad situatyvinę teoriją galima laikyti pozityvistine, kadangi ši teorija remiasi empiriniais duomenimis. Teorijoje egzistuoja požiūris, kad, siekiant didinti organizacijos efektyvumą, yra būtina nagrinėti konkrečias analogiškas situacijas ir parengti tipinius šių situacijų sprendimus, kurie gali būti taikomi ateityje. Nagrinėjant konkrečias situacijas, yra būtina išskirti vidaus ir išorės veiksnius, kurie gali veikti organizaciją. Tiriant vidaus veiksnius, yra nustatoma konkrečių posistemių įtaka konkrečiai susidariusiai situacijai bei visų šių poveikį turinčių posistemių įtakos sujungimo galimybes. Tiriant išorinius veiksnius, būtina atsižvelgti į galimai atsirasiančius šių veiksnių neapibrėžtumus. Kibernetinio saugumo kontekste šis vidinių ir išorinių veiksnių tyrimas taip pat yra būtinas, kadangi asmenys, vykdantys kibernetinius išpuolius, nuolat keičia ir modifikuoja savo puolimo priemones ir metodus. Iš pažiūros panašios atakos gali turėti visiškai skirtingus veikimo vektorius ir siekti visiškai skirtingų tikslų (Craig, Valeriano, 2016; Kovacich, 2016; Limba ir kt., 2017).

Vertinant situatyvinės teorijos pritaikomumo kibernetinio saugumo valdymo galimybes, galima teigti, kad ir H. Fajolio, ir M. Vėberio, ir E. Majo teorijos, ir ši teorija gali būti pritaikomos kibernetiniam saugumui valdyti, bet tas pritaikomumas turi tam tikrų apribojimų, kurie gimsta iš pačios kibernetinio saugumo dinamiškumo problemos. Kibernetinių pažeidžiamumų gausa ir jų kitimo greitis bei naujų metodų ir būdų atsiradimas sukelia problematiką, kuri slypi standartinių situacijų nagrinėjimo aspekte: situacija dažnai keičiasi greičiau nei galima ją įvertinti ir aprašyti.

T. Burn ir G. M. Stalker buvo vieni pirmųjų mokslininkų, kurie teigė, kad organizaciją veikianti aplinka apsprendžia organizacijos požymius (Burns, Stalker, 1961). Šie mokslininkai teigė, kad mechanistinė organizacija, kuri veikia stabilioje aplinkoje ir

orientuojasi į procedūras, turi galimybę pasiekti didžiausią savo efektyvumą (Mechanistinė organizacija gali būti traktuojama kaip organizacija, savo veikloje naudojanti M. Vėberio modelį). Stabili aplinka sąlygoja organizacijos galimybes:

- išmokti veikti, optimizuojant savo efektyvumą;
- suvokti organizacijos išteklių panaudojimo efektyvumo klausimą;
- pasiekti didžiausią galimą savo veiklos pelną.

Kaip jau ir buvo kalbama anksčiau, kibernetinį saugumą nagrinėjant organizacijos struktūros dimensijoje, galima naudoti M. Vėberio sukurtą organizacijos modelį, nes kibernetinio saugumo dinamiškumas sukelia tam tikrus aplinkos stabilumo svyravimus, šis modelis gali turėti tam tikrų įgyvendinimo problemų.

Nuolat besikeičianti ir nestabili aplinka mechanistinei organizacijai kelia egzistavimo problemą. Mechanistinė organizacija nesugeba nedelsdama reaguoti į aplinkos pokyčius ir jos veikla tampa nestabili. Dėl šios priežasties organizacija turi būti organiška, sugebanti greitai ir sėkmingai adaptuotis prie besikeičiančios aplinkos.

Neapibrėžtumų teorijos kūrėjai teigė, kad aplinkos neapibrėžtumas yra lemiantis veiksnys, paaiškinantis specifinių organizacijų formų sėkmę, o neapibrėžtumas aplinkoje buvo apibūdintas kaip sąveika tarp kompleksiškumo ir pokyčių tempo. Kompleksiškumas yra apibūdinamas kaip skirtingų poveikio elementų kiekis aplinkoje, o pokyčių tempas parodo, koks yra aplinkos, sudarytos iš visų jos elementų, kaitos greitis.

Taigi, galima drąsiai teigti, kad kibernetinio saugumo srityje mechanistinė organizacija yra pasmerkta žlugti. Organizacijos struktūra turi būti lanksti, o pati organizacija turi mokėti greitai prisitaikyti prie ją supančios aplinkos. Žinant, koks dinamiškas yra kibernetinio saugumo valdymas, kaip greitai ir netikėtai keičiasi ši technologinė sritis, galima aiškiai numatyti, kad ir pačios organizacijos struktūra bus dinamiška (Sheymov, 2016; Singh, 2018; Petuchov, Gusnin, 2019), su tam tikrais statiniais elementais, o vadovavimas organizacijoje priklausys nuo organizacijos sąveikos ir aplinkos situacinio santykio. Laikantis tokio požiūrio, organizacijos vadovų ir visos organizacijos veikla tam tikrais sprendimų priėmimo momentais turės būti lankstesnė bei adaptuota prie susidariusios situacijos (Evans ir kt., 2016; Limba ir kt., 2017; Houston, 2019).

Apibendrinant šį skirsnį, būtina pažymėti, kad kibernetinio saugumo valdymas yra labai dinamiškas ir greitai besikeičiantis dalykas. Sparčiai kintanti aplinka, atsirandančios naujos įsibrovimų technologijos ir naujos grėsmių rūšys verčia valstybes susimąstyti apie šios srities valdymą, bet dabartiniu momentu atliktas labai ribotas skaičius mokslinių tyrimų, nagrinėjant šią sritį ne iš technologinės, o iš valdymo pozicijos.

Didžiausia problema yra ta, kad kibernetinis saugumas yra suprantamas kaip technologijos mokslas ir beveik nėra kreipiamas dėmesys į tai, kad prieš bet kokių technologijų diegimą turi būti iš esmės atlikti moksliniai tyrimai, nusakantys tų technologijų naudojimo ir valdymo galimybes. Turi būti aiškiai apibrėžiama, kokios organizacijos ir kokiais būdais vykdys kibernetinį saugumą, nusakoma tų organizacijų vidinė struktūra, pavaldumo hierarchija, darbų pasidalinimas bei atsakomybės ir atskaitomybės ribos.

Nagrinėjant kibernetinį saugumą valstybės kontekste, būtina vertinti tris dimensijas: struktūrų dimensiją, santykių dimensiją ir aplinkos dimensiją. Panaudojant šias tris dimensijas, galima sukurti gerai veikiančią organizaciją, kuri galės ne tik tinkamai

veikti jau egzistuojančioje aplinkoje, bet ir greitai prisitaikyti prie nuolat besikeičiančios aplinkos, nes nuolatinė kaita yra vienas iš kibernetinio saugumo iššūkių.

Struktūrų dimensijoje, kuriant kibernetinį saugumą valdančią organizaciją, gali būti naudojami M. Vėberio ir H. Fajolio pasiūlyti organizacijų modeliai, bet šiuos modelius būtina adaptuoti ir į organizacijos veiklos procesus žiūrėti šiek tiek nuolaidžiau. Organizacija turi gebėti savo veikloje naudoti ne tik universalistinį požiūrį į valdymą, bet ir atsižvelgti į tam tikrus valdyme egzistuojančius partikuliarizmo aspektus.

Vidinių santykių dimensijoje turi būti derinami klasikinės ir žmogiškųjų santykių teorijų nuostatos. Mechaninis požiūris į žmogų kaip į darbo įrankį galimas tik tais atvejais, kai organizacija veikia pagal jau žinomus ir patvirtintus scenarijus, o atsiradus naujoms aplinkybėms ar neaiškioms situacijoms, turi būti naudojamas kolegialus valdymas.

Aplinkos poveikio dimensijos perspektyvoje taip pat turi būti naudojamas sisteminis požiūris į organizaciją. Organizacija gali veikti pagal situacinį modelį, kai yra visiškai aiškios ir pasikartojančios aplinkybės, bet kai aplinkos situacija tampa neaiški, organizacijos veikla turi būti vykdoma pagal aplinkos neapibrėžtumo teorijos nuostatas.

Pažymėtina, kad kibernetinio saugumo valdyme vadovui negalima pasinerti į kraštutinumus: nustatyti stabilius ir nekintančius organizacijos rėmus, bet tuo pačiu metu negalima visko paleisti iš rankų ir visus sprendimus perduoti kolektyviniams sprendimams. Vadovai tokioje organizacijoje privalo derinti *kietą ir minkštą valdymą*.

Gerosios valdymo praktikos, naudojamos verslo organizacijose, taip pat gali būti perkeliamos į šią sritį, bet būtina nepamiršti, kad ne visi verslo naudojami valdymo principai gali būti pritaikomi viešojo sektoriaus veikloje, o kartais verslininkiškumas yra visiškai nepritaikomas valstybei. Perkeliant tam tikras praktikas iš verslo į valstybės valdymo sritį, šis perkėlimas turi būti labai gerai apgalvotas, o paprastas mechaninis šių principų perkėlimas į viešąjį sektorių yra negalimas.

Kibernetinio saugumo gerinimas valstybėje gali atnešti dvigubos naudos: bus sprendžiamas tinkamas valstybės infrastruktūros ir kitų išteklių panaudojimas bei apsauga, bus didinamas dabartiniu metu gyventojams teikiamų viešųjų paslaugų saugumas. Didinant gyventojų pasitikėjimą valstybės teikiamomis elektroninėmis paslaugomis, gyventojai bus netiesiogiai skatinami labiau pasitikėti ir elektroninio balsavimo sistemomis, kurių saugumas kelia gyventojams daug klausimų. Stiprinant saugumą, sustiprės ir gyventojų pasitikėjimas balsavimo sistemomis. Taip gyventojai bus paskatinti aktyviau dalyvauti tiesioginiame valstybės valdyme, o tai ypač akcentuojama naujojo viešojo, gerojo ir sumanaus valdymo paradigmose.

1.2. Kibernetinių incidentų atsiradimo priežastis ir valdymo problematika

Kibernetiniai nusikaltėliai, vykdydami nusikaltimus, dažniausiai sutelkia savo pastangas į ypatingos svarbos (kritinės) infrastruktūros atakas, nes sėkmingo išpuolio atveju šios atakos tikėtina suteiks finansinį ar politinį „pelną“. Šią situaciją sąlygoja kritinės infrastruktūros sistemų sandaros ypatumai: kritinėje infrastruktūroje, kaip ir kitose informacinėse sistemose, yra naudojami komerciniai produktai (programinė ir

techninė įranga, komunikaciniai sprendimai ir ryšio kanalai) (Anderson, 2001), o kibernetiniai nusikaltėliai, turėdami tam tikrų technologinių žinių apie kritinėje infrastruktūroje naudojamų informacinių ir telekomunikacinių technologijų sprendimus, gali išnaudoti naudojamų technologinių komercinių produktų pažeidžiamumus siekdami sutrikdyti normalų sistemų darbą, pakeisti arba sunaikinti informaciją, kuri yra naudojama sistemos viduje (US GAO, 2005; US Department of Energy, 2006; Bologna ir kt., 2013).

Pažymėtina, kad tokia situacija yra susidariusi dėl organizacijų ir visuomenės besąlygiško pasitikėjimo informacinėmis ir ryšių technologijomis. Būtent pasitikėjimas technologijomis ir neteisingas jų panaudojimas dažniausiai sąlygoja kibernetinius išpuolius prieš kritinę infrastruktūrą, o patys išpuoliai dažniausiai paveikia labai platų gyventojų ir organizacijų ratą. Pavyzdžiui, Estijoje 2007 metų pavasarį įvyko masinės, tris savaites trukusios kibernetinės atakos (kartais šios atakos vadinamas pirmuoju kibernetiniu karu) arba 2015 metais įvyko išpuolis prieš Ukrainos elektros energijos tiekimo sistemą. Estijoje dėl kibernetinių atakų buvo sutrikusi žiniasklaidos, valstybės institucijų ir bankinio sektoriaus veikla, o Ukrainoje 225 000 vartotojų buvo nutrauktas energijos tiekimas. JAV Valstybės saugumo departamentas (*angl. US Department of Home Security*) pareiškė, kad kibernetinė ataka Ukrainoje buvo vykdoma, pasitelkiant kenkėjišką (*angl. malicious*) programinę įrangą, o šis kibernetinis incidentas tikriausiai yra pirmasis žinomas atvejis, kai kibernetinis įsibrovimas į kritinę infrastruktūrą nutraukė energijos tiekimo paslaugas dideliam kiekiui vartotojų. Buvo daug bandymų surasti šio kibernetinio išpuolio iniciatorius, tačiau viena iš kibernetinių incidentų tyrimo problematikų slypi tame, kad elektroninėje erdvėje kyla atsakomybės priskyrimo problema – yra labai sunku atsekti tikrus įvykio iniciatorius ir vykdytojus (Volz, 2016).

Manytina, kad geriausia priemonė, siekiant užkirsti kelią kibernetinių incidentų atsiradimui, yra visapusiškas kibernetinio saugumo gerinimas. Tačiau akcentuotina yra ir kibernetinio saugumo incidentų prigimtis, kuri sąlygoja labai sunkų jų nuspėjimą, aptikimą ir valdymą (prevencinių priemonių naudojimą). Dėl šios priežasties didėja rizika, kad kibernetiniai įsibrovimai gali būti sėkmingai įgyvendinami, o pačių išpuolių kiekis, kaip matoma iš pasaulinės kibernetinių incidentų statistikos, tendencingai didėja (CERT-UK, 2015; Federal Office for Information Security, 2016; statista.com, 2018).

Pažymėtina, kad ne vien tik kibernetinių incidentų prigimtis yra viena iš pagrindinių kibernetinio saugumo mažėjimo priežasčių: ne visos pasaulio šalys yra parengusios reagavimo į kibernetinius incidentus planus, kurie nusako veiksmus ir atsaką į kibernetines atakas bei numato veiksmus, susijusius su kibernetinių pažeidžiamumų vertinimu ir mažinimu. Reikėtų pažymėti, kad paprasti technologiniai sprendimai (techninė ir programinė įranga) neišsprendžia visų kibernetinio saugumo problemų, susijusių su kritinės infrastruktūros apsauga (Cayirci, Ghergherehchi, 2011), bet esminės problemos gali būti sprendžiamos, įgyvendinant kibernetinio saugumo valdymo modelį, kuris turi būti tobulinamas, atsižvelgiant į sparčiai besikeičiančias technologijas, teisinį reguliavimą ir kitus aspektus (Limba ir kt., 2016). Kritinės infrastruktūros saugumo situacijos kitimas yra siejamas su verslo praktikų (Kiškis ir kt., 2016), rinkos tendencijų (Kiškis, Limba, 2016) ir pasaulyje naudojamų technologijų (Vlasenko ir

kt., 2016) kaita, kuri, savo ruožtu, reiškia ir būtinybę keisti požiūrį į kritinės infrastruktūros valdymą, ir jos atsparumo kibernetiniams pažeidžiamumams didinimą. Mokslininkai K. Barnes, B. Johnson ir R. Nickelson pažymi, kad kibernetiniai pažeidžiamumai yra linkę kilti toje infrastruktūros vietoje, kurioje egzistuoja didžiausia prisijungimo (prieigos) galimybė, o šios prisijungimo galimybės kontrolė yra silpniausia (Barnes ir kt., 2004). Mokslininkai išskiria keturias kibernetinių pažeidžiamumų sritis (domenus). Kiekvienai iš jų yra būdingi savo atakos vektoriai, kuriuos savo tikslams pasiekti naudoja kibernetiniai nusikaltėliai:

- informacinių technologijų (toliau – IT) sritis;
- informacinių ir ryšių technologijų (toliau – IRT) sritis;
- komunikacijų sritis;
- fizinės prieigos sritis.

Šiandieniniame pasaulyje, kurį keičia nesustabdoma technologijų plėtra, IT ir IRT domenai negali egzistuoti atskirai, todėl galima teigti, kad šiuolaikinėje infrastruktūroje šių domenų komponentai yra sujungti į vieną bendrą visumą (Masero, 2010).

Apibendrinant galima išskirti keturias pagrindines priežastis, kurios sąlygoja kibernetinių incidentų atsiradimą: technologinis progresas ir sparčiai besikeičianti pasaulinė technologinė pažanga, kuri sudaro galimybę kibernetiniams nusikaltėliams pasiekti didesnį potencialių aukų skaičių; techninės ir programinės įrangos, naudojamos kritinėje infrastruktūroje, netobulumas ir ne pilnas suderinamumas, kuris technologiškai apriboja ar sumažina kibernetinio saugumo priemonių panaudojimo galimybes; netobulas kibernetinį saugumą reglamentuojančių dokumentų (teisės aktų, reagavimo ir atstatymo po incidentų planų) parengimas; kibernetinių incidentų atsiradimo, nustatymo ir valdymo problematika.

Kaip jau buvo minėta anksčiau, kibernetinio saugumo incidentų prigimtis sudaro galimybes sėkmingai vykdyti kibernetines atakas į, kadangi kibernetinius incidentus yra sunku numatyti, aptikti ir valdyti (Craig, Valeriano, 2016). Kibernetinis saugumas taip pat turi būti suprantamas kaip reiškinys, kuris peržengia įprastą informacijos saugumo apibrėžimą, grindžiamą CIA triada: informacijos konfidencialumas, integralumas ir autentiškumas. Pažymėtina, kad paprasti technologiniai sprendimai gali būti naudojami CIA triados sritims užtikrinti, bet kibernetinis saugumas yra daug sudėtingesnis reiškinys ir jam užtikrinti reikalingas daug platesnis požiūris. Būtent tai sąlygoja didesnį šio reiškinio nesupratimą visuomenėje ir organizacijų viduje (Johnson, 2015). Toliau bus aptariamos penkios dažniausiai pasitaikančios klaidos, kurias organizacijos daro, vertindamos savo valdomos kritinės infrastruktūros kibernetinį saugumą:

- *Apgaulingas manymas, kad bet kurią infrastruktūrą galima visiškai apsaugoti nuo įsibrovimų ir kibernetinių grėsmių*. Bet kuri organizacija (viešojo ar privataus sektoriaus atstovai) ar jos struktūrinis padalinys, valdantys informacinių išteklių infrastruktūrą, o ypač kritinę infrastruktūrą, turi aiškiai suvokti, kad visiškas kibernetinis saugumas yra mitas arba, tiksliau sakant, – nepasiekiama svajonė (Limba ir kt., 2017). Pats svarbiausias kibernetinio saugumo iššūkis yra aiškiai suklasifikuoti ir suprasti, kokia organizacijos infrastruktūra yra labiausiai pažeidžiama bei kokių veiksmų privalu imtis, kad būtų išvengta grėsmių. Taip pat turi

būti vienareikšmiškai įvardijami technologiniai mechanizmai (techninė ir programinė įranga), kurie leistų aptikti neįprastą aktyvumą infrastruktūroje, bei planai, kurie aprašo, kokiais veiksmais galima suvaldyti galimai kilsiančius kibernetinius incidentus, sumažinti šių incidentų sukeltus praradimus (nuostolius) bei atstatyti normalų infrastruktūros veikimą (WISAC, 2015). Tačiau esminis aspektas, kuris turėtų būti svarbiausias organizacijoje – kritinių situacijų nustatymas ir reagavimas į jas, nes būtent tai suteikia galimybę stipriai sumažinti nuostolius, susijusius su kibernetinio saugumo pažeidimais (Techrepublic, 2004);

- *Klaidingas manymas, kad, įdarbinant geriausius kibernetinio saugumo ekspertus ar informacinių sistemų specialistus, pavyks išvengti kibernetinių incidentų*. Labai svarbu, kad organizacijos vadovai ir personalas suprastų, jog kibernetinis saugumas nėra specialistai ar departamentas organizacijos viduje, o visos organizacijos ir jos narių požiūris (Singer, Friedman, 2014; WISAC, 2015; Limba ir kt., 2017). Manymas, kad kibernetinis saugumas yra departamentas ar jame dirbantys specialistai, suteikia organizacijai apgaulingą kibernetinio nepažeidžiamumo jausmą, kuris yra iš esmės klaidingas, kaip jau buvo minėta anksčiau. Kibernetinis saugumas turi būti suprantamas kiekvienam organizacijos nariui ir būti kiekvieno organizacijos nario siektinu tikslu, kadangi žmogus (žmogiškasis faktorius) yra pats pažeidžiamiausias elementas kibernetinio saugumo prasme (Techrepublic, 2004; Wei ir kt., 2010). Toks požiūris leis organizacijai sėkmingai pasirūpinti savo kibernetiniu saugumu, o visi organizacijos nariai gali būti skatinami piniginėmis išmokomis, jei prisidės prie šios organizacijos politikos kūrimo ir palaikymo;
- *Organizacijose naudojamų kibernetinio saugumo technologinių priemonių (techninės ir programinės saugumo įrangos) pervertinimas ir per didelis pasitikėjimas jomis*, užtikrinant valdomos infrastruktūros naudojimą. Komercinės įmonės, gaminančios techninę ir programinę įrangą, niekada negarantuos jų gaminamos produkcijos nepažeidžiamumo ir šimtaprocentinės jūsų organizacijos apsaugos nuo kibernetinių grėsmių. Šiuolaikiniame pasaulyje naudojamos saugumo technologijos ir įrankiai yra kuriami tam tikrai siaurai kibernetinio saugumo sričiai užtikrinti (neįprastam duomenų srautų judėjimui telekomunikaciniame tinkle, kenkėjiškos programinės įrangos veiklai ar įsibrovimui aptikti) ir dažniausiai nėra skirti kompleksinei viso duomenų perdavimo tinklo kibernetinio saugumo analizei atlikti, bet šios priemonės ir jų rinkiniai būtinai turi būti naudojami, siekiant apriboti pažeidžiamumų skaičių bei galimų kibernetinių nusikaltėlių veiksmus (Techrepublic, 2004; Wei ir kt., 2010, Limba ir kt., 2017). Įrankių reikalingumas ir naudojimas turi būti apgalvotas ir pasvertas. Tai turi būti atlikta tik po to, kai kibernetinio saugumo kryptys ir koncepcijos organizacijoje yra aiškiai suprantamos ir apibrėžtos, o kiekvienas organizacijos narys supranta kibernetinio saugumo svarbą, nes, kaip ir buvo minėta anksčiau, silpniausią grandį sudaro žmogiškasis faktorius, o įsibrovėliai tai puikiai žino ir tuo naudojasi. Žmogiškasis faktorius kibernetiniame saugume gali būti veikiamas, bet organizacijos vadovai turi prisiimti atsakomybę, spręsdami šią problemą.

Organizacijoms reikia suprasti, kad kiekvienas įmonės darbuotojas turi tobulėti ir aiškiai suvokti kibernetinių išpuolių sukeliamą grėsmę;

- Klaidinga nuomonė, kad *kibernetinis saugumas yra tiesioginis infrastruktūros sutrikimų ir neįprasto infrastruktūros veikimo stebėjimas*. Kibernetinio saugumo stebėjimas neapsiriboja vien tik naudojamų technologinių priemonių ir infrastruktūros veiklos stebėjimu. *Stebėjimas* kibernetinio saugumo kontekste yra siejamas su platesniu požiūriu į valdomą infrastruktūrą ir vertinamas kaip išorinės ir vidinės organizacijos kibernetinės aplinkos santykis: tarpusavyje yra susiejamos konkrečių organizacijos valdomų informacinių sistemų, infrastruktūrų veikla, infrastruktūroje vykstančių kibernetinių incidentų vertinimas, išorinės aplinkos kibernetinės situacijos vertinimas ir kibernetinio nusikalstamumo tendencijų stebėjimas (Limba ir kt., 2017). Stebėjimas yra bevertis, jei surinktų duomenų negalima panaudoti tolimesnėms prognozėms atlikti ar įvertinti ateityje galinčias kilti rizikas (WISAC, 2015). Jei organizacija sugebės suprasti išorinės aplinkos kibernetinio saugumo pokyčius ir tų pokyčių tendencijas bei sugebės pasinaudoti šiomis įžvalgomis, tai įgalins organizaciją parengti tinkamas ateities kibernetinio saugumo gaires ir strategijas, kurias ateityje bus galima sėkmingai panaudoti kovoje su kibernetiniais incidentais. Kitaip tariant, ateities organizacijos kibernetinio saugumo politika ir strategija turi būti grindžiama nuolatiniu organizacijų mokymusi ir plėtra, o ateities grėsmių supratimas suteiks galimybes pasirengti būsimoms grėsmėms. Toks organizacijų naudojamas metodas yra ir žymiai efektyvesnis piniginių sąnaudų atžvilgiu, nes jis turi tam tikrų pranašumų prieš trumpalaikį kibernetinio saugumo padidinimo metodą, kai, bandant apsisaugoti, bet neturint aiškios galutinės kibernetinio saugumo vizijos, diegiami skirtingi technologiniai sprendimai, kartais nelabai derantys tarpusavyje. Taip pat svarbu, kad būtų užtikrintas tarporganizacinis dialogas, kai organizacijos turima informacija apie kibernetinio saugumo pažeidžiamumus ir incidentus dalijasi tarpusavyje, nes tik keitimasis informacija gali padėti sukurti bendrą vaizdą apie faktinę saugumo situaciją mieste, regione, valstybėje ar pasaulyje (Govindarasu, Hanas, 2017);
- Klaidinga nuomonė, kad *kibernetinio saugumo priemonės, kurios yra naudojamos kritinei infrastruktūrai nuo vidinių ir išorinių kibernetinių grėsmių apsaugoti, yra daugiau nei pakankamos, nevertinant aplinkos*. Pirmiausia būtina nustatyti, koks kibernetinio saugumo lygis yra priimtinas organizacijai, ir tik po to vertinti priemones, kurios padės pasiekti užsibrėžtą tikslą. Veiksmingas kibernetinis saugumas ir bandymas išvengti kibernetinių grėsmių ir atakų gali būti palyginamas su maratono varžybomis, kuriose vienas dalyvis pirmauja (kibernetinis nusikaltėlis), o kiti stengiasi jį pavyti (kibernetinio saugumo ekspertai). Kibernetiniai nusikaltėliai, vykdydami savo veiklą, kuria naujus metodus ir technikas, o saugumo ekspertai visada vienu žingsniu atsilieka. Atrodo, kad yra naudinga investuoti į vis sudėtingesnes saugumo priemones, kad būtų užkirstas kelias kibernetiniams incidentams, tačiau tikrovė yra šiek tiek kitokia. Pagal kibernetinio saugumo politiką pirmenybė turi būti teikiama investicijoms į ypatingos svar-

bos (kritinę) infrastruktūrą ir išteklius, o ne į naujausias technologijas ar sistemas, galinčias aptikti bet kokią grėsmę (WISAC, 2015). Organizacijoms būtina suprasti, kokie įsibrovėliai gali būti suinteresuoti organizacijos veikla ir kodėl. Vėliau būtina įvertinti savo valdomus išteklius ir, atsižvelgiant į atliktą vertinimą, prisiimti tam tikrą pažeidžiamumo riziką, nes, kaip buvo minėta anksčiau, neribotos investicijos į technologijas neužtikrina visiško organizacijos valdomos infrastruktūros kibernetinio saugumo (Limba ir kt., 2017).

Pažymėtina, kad visos anksčiau paminėtos organizacijų klaidos, vertinant savo kritinės infrastruktūros kibernetinį saugumą, yra dažnai pasitaikančios kaip privačiojo, taip ir viešojo sektoriaus organizacijose, tačiau jų sprendimas turi būti atliekamas sistemingai ir apgalvotai, turint tam tikrą galutinį tikslą. Pagrindinė ir dažniausia klaidų atsiradimo priežastis yra ta, kad kibernetinis saugumas organizacijoje yra traktuojamas ne kaip pagrindinis organizacijos tikslas, o kaip jos vykdomos veiklos pridėtinė dalis. Dažnai kibernetinio saugumo ekspertai į organizacijos veiklą yra įtraukiami tik tuomet, kai organizacijoje jau yra susikūrę ir nusistovėję tam tikri veiklos procesai ir keisti visos organizacijos veiklą yra labai sudėtinga. Toks požiūris į kibernetinį saugumą yra ydingas (Limba ir kt., 2017).

Kibernetinis saugumas turėtų būti visų naujų technologinių sprendimų ir sistemų kūrimo kertinis akmuo, o dabar dažnai atsitinka taip, kad apie jį pagalvojama tik projekto pabaigoje. Taip įvyko su interneto architektūra, kuri buvo sukurta, siekiant skatinti ryšį, o ne saugumą (Jenab, Moslehpour, 2016).

1.3. Kibernetinio saugumo valdymo modelių analizė

Kibernetinio saugumo valdymas šiuolaikinėje organizacijoje yra sudėtingas ir daug resursų reikalaujantis dinaminis procesas, kuris dažnai nėra aiškiai suprantamas organizacijos vadovų ir organizacijos narių (Johnson, 2015; Dalzien, 2016). Per pastaruosius du dešimtmečius buvo sukurta daugybė kibernetinio saugumo valdymo sistemų (modelių, gairių, standartų, priemonių, technologijų ir kt.), kurios yra naudojamos organizacijose, kuriant jų kibernetinį saugumą (ISO/IEC, 2013; US-CERT, 2018; $(ISC)^2$, 2015; SANS, 2018).

Šiame disertaciniame darbe nagrinėjant pasaulyje egzistuojančias kibernetinio saugumo valdymo sistemas (gaires, standartus, priemones ar technologijas) jos yra traktuojamos kaip modeliai, kurie yra tam tikros realios sistemos abstrakcija, su jų autorių numatytomis savybėmis, kurios yra svarbios sprendžiamai problemai.

Visos siūlomos kibernetinio saugumo valdymo sistemos nėra privalomos įdiegti, bet organizacija, kuri rūpinasi savo kibernetiniu saugumu, gali pasinaudoti tarptautiniu lygiu pripažintų valstybinių institucijų ir verslo kompanijų parengtomis metodikomis ir įgyvendinti kibernetinio saugumo valdymo gaires savo veikloje. Pažymėtina, kad anksčiau minėtos kibernetinio saugumo valdymo metodikos nėra orientuojamos į technologinius procesus ir konkrečią techninę ar programinę įrangą, kuria užtikrinamas kibernetinis saugumas organizacijoje. Kibernetinio saugumo valdymas anksčiau minėtose valdymo gairėse yra orientuotas į saugumo pažeidžiamumų, rizikos

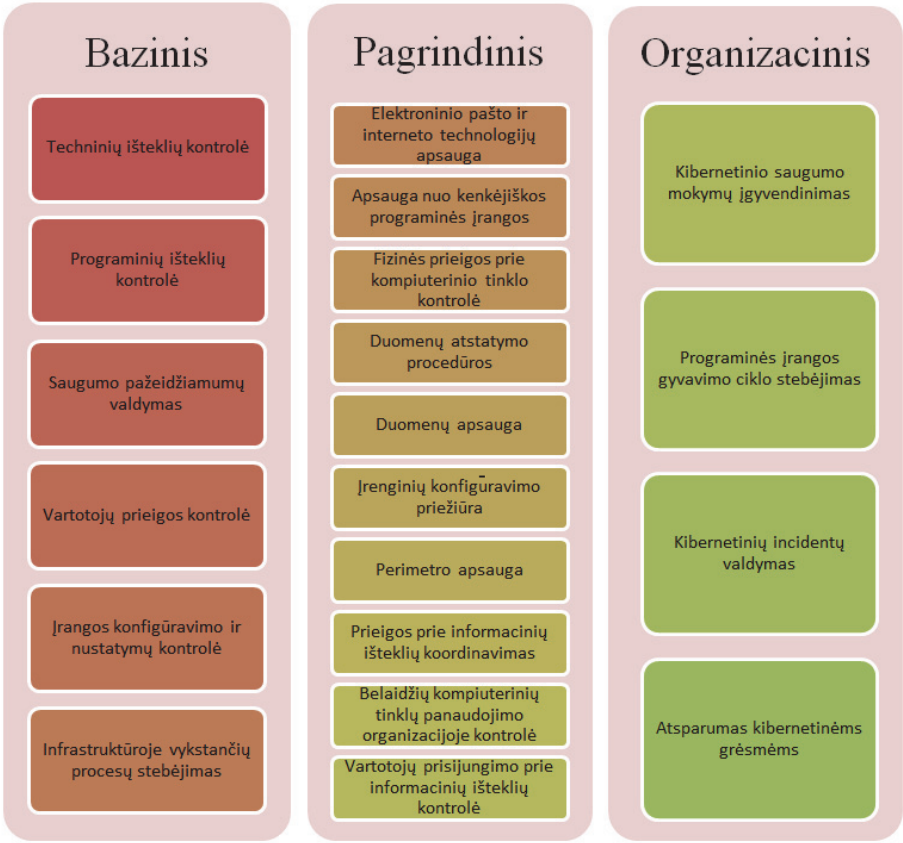
vertinimo ir technologijų įdiegimo procesų valdymą. Pažymėtina, kad organizacijoms siūlomos kibernetinio saugumo valdymo sistemos nėra statinės ir jas parengusios kompanijos ir valstybinės organizacijos nuolat atnaujina savo parengtas kibernetinio saugumo valdymo gaires, atsižvelgdamos į kibernetinio saugumo situaciją pasauliniame kontekste, technologijų raidą, kibernetinių pažeidžiamumų ir atakų raidos pokyčius (Donaldson ir kt., 2015).

1.3.1. SANS kibernetinio saugumo kontrolės priemonių valdymo modelis

2018 metais SANS institutas, bendradarbiaudamas su informacinių technologijų ir kibernetinio saugumo ekspertais, atnaujino savo 2013 metais parengta kibernetinio saugumo valdymo metodiką, kuri savyje sujungė geriausias pasaulines praktikas, siejamas su kibernetinio saugumo valdymu organizacijose, vykdančiose savo veiklą gamybos, farmacijos, viešajame sektoriuje, gynybos ir kitose srityse. SANS institutas pažymi, kad egzistuoja penki esminės veiksmingos kibernetinės gynybos sistemos principai (SANS, 2018), kuriais yra grindžiama visa instituto parengta kibernetinio saugumo valdymo sistema:

- *Gynybinių mechanizmų parinkimas* – gynybos technologijos ir mechanizmai yra parenkami, atsižvelgiant į piktavalių naudojamas kibernetines atakas, o žinios apie atakas, kurios paveikė realiai egzistuojančias kompiuterines sistemas, užtikrina organizacijoms galimybę tobulėti ir kurti veiksmingą kibernetinės gynybos sistemą;
- *Prioritetų nustatymas* – pirmenybė investuojant teikiama technologijoms ir priemonėms, kurios užtikrins didžiausią rizikos mažinimą ir apsaugą nuo pavojingiausių faktorių, egzistuojančių organizacijos infrastruktūroje, atsižvelgiant į šių priemonių įgyvendinimo galimybę organizacijos aplinkoje;
- *Vertinimo sistemos nustatymas* – bendros, visiems suprantamos vertinimo sistemos įdiegimas ir naudojimas organizacijoje suteiks organizacijos nariams galimybę vienodai vertinti organizacijos naudojamų saugumo priemonių veiksmingumą bei paspartins reikalingų pakeitimų nustatymo ir įgyvendinimo procesą;
- *Nuolatinis situacijos vertinimas ir grėsmių mažinimas* – organizacijoje yra būtina įdiegti nuolatinį kibernetinio saugumo situacijos stebėjimo ir vertinimo procesą, kuris leis stebėti bei vertinti organizacijoje naudojamų ir naujai diegiamų kibernetinio saugumo valdymo priemonių efektyvumą, sudarant sąlygas mažinti kibernetines grėsmes;
- *Apsaugos priemonių automatizavimas* – automatizuotos kibernetinio saugumo valdymo priemonės ir technologijos suteiks organizacijai galimybę atlikti kibernetinio saugumo situacijos vertinimą, pasinaudojant nekintamais, išmatuojamais ir patvirtintais kriterijais, tuo pačiu metu suteikiant organizacijai galimybę eliminuoti žmogiškųjų klaidų įtaką kibernetinio saugumo vertinimo procese.

SANS instituto kibernetinio saugumo valdymo modelis detalizuoja dvidešimt kibernetinio saugumo valdymo sričių, kuriose kibernetinio saugumo valdymo priemonių ir technologijų įgyvendinimas yra būtinas, norint sukurti tvarų organizacijos kibernetinio saugumo valdymo modelį. SANS instituto parengto kibernetinio saugumo valdymo modelio domenai ir jų valdymo sritys grafiškai pavaizduojamos 2 paveiksle.



Šaltinis: *SANS, 2018*

2 paveikslas. *SANS kibernetinio saugumo valdymo domenai*

Visas kibernetinio saugumo valdymo modelis yra suskirstytas į tris domenus, kurie, pasak kibernetinio saugumo valdymo modelio kūrėjų, užtikrins visišką kibernetinio saugumo valdymo įgyvendinimą organizacijoje (SANS, 2018):

1. *Bazinis* (*angl. basic*) domenas, sujungiantis naudojamų techninių ir programinių išteklių kontrolę; saugumo pažeidžiamumų valdymą; vartotojų prieigos prie informacinių išteklių kontrolę; techninės ir programinės įrangos, naudojamos organizacijos infrastruktūroje, konfigūravimo ir nustatymų kontrolę; infrastruktūroje vykstančių procesų valdymą ir stebėjimą;
2. *Pagrindinis* (*angl. foundational*) domenas, kuriame nagrinėjamos elektroninio pašto ir interneto technologijų apsaugos priemonės; apsauga nuo kenkėjiškos programinės įrangos; fizinės prieigos prie organizacijos naudojamo kompiuterinio tinklo organizavimas ir kontrolė; duomenų apsauga ir duomenų atstatymas; kompiuterinio tinklo įrenginių konfigūravimas; perimetro apsauga; prieigos prie

informacinių išteklių koordinavimas; belaidžių kompiuterinių tinklų panaudojimas organizacijos infrastruktūroje; vartotojų prisijungimo prie informacinių išteklių organizavimo ypatumai;

3. *Organizacinis* (*angl. organizational*) domenas, nagrinėjantis kibernetinio saugumo mokymų įgyvendinimą organizacijoje; organizacijos infrastruktūroje naudojamos programinės įrangos gyvavimo ciklo stebėjimą; kibernetinių incidentų valdymą; organizacijos atsparumo kibernetinėms grėsmės tikrinimą.

Pažymėtina, kad visi trys SANS instituto kibernetinio saugumo valdymo domenai yra glaudžiai susiję tarpusavyje, todėl organizacija, siekdama įdiegti šį kibernetinio saugumo valdymo modelį, turi tai daryti laipsniškai: pirmiausia turi būti skiriamas dėmesys baziniam domenui, kuris SANS instituto yra vadinamas *kibernetine higiena* (*angl. cyber hygiene*) (SANS, 2018), o tik po to, kai organizacija pasiekia tam tikrą brandos lygį, gali būti nuosekliai pereinama prie pagrindinio ir organizacinio domenų saugumo sričių įgyvendinimo.

SANS valdymo modelyje kibernetinis saugumas labiausiai nagrinėjamas kaip tarpusavyje susiję technologiniai procesai (technologinis aspektas), t. y. pateikiamas organizacijai būtinų atlikti veiksmų sąrašas, kuris užtikrins technologinį kibernetinį saugumą organizacijos informaciniuose ištekliuose. Tačiau modelyje yra pažymima žmogiškojo faktoriaus svarba, užtikrinant kibernetinį saugumą: aprašomas žmogiškųjų išteklių valdymas, siekiant suteikti organizacijai gebėjimą sėkmingai identifikuoti, lokalizuoti ir valdyti kibernetinius saugumo incidentus (pvz., darbuotojų mokymas, personalo atsakomybių nustatymas, kibernetinių incidentų valdymo taisyklės, kibernetinio saugumo pratybos ir kt.). Reikia atkreipti dėmesį į tai, kad modelis nenagrinėja tokių svarbių kibernetinio saugumo aspektų kaip: rizikų identifikavimas ir valdymas; organizacijos išorinės kibernetinio saugumo aplinkos stebėjimas; organizacijos vidinių tvarkų ir taisyklių atitiktis teisiniam reglamentavimui.

1.3.2. NIST kritinės infrastruktūros kibernetinio saugumo sistema

Pasaulio valstybių gerovė priklauso nuo patikimo ir nepertraukiamo ypatingos svarbos infrastruktūros objektų funkcionavimo ir kibernetinio saugumo (Sofiou, 2019). Kibernetiniai nusikaltėliai, siekdami savo tikslų, išnaudoja kibernetines grėsmes ir pažeidžiamumus, pasinaudodami ypatingos svarbos infrastruktūros sistemų sudėtingumu ir kompleksiškumu, bei savo veiksmais sukelia pavojų visos valstybės gyventojų saugumui ir sveikatai bei valstybės ekonomikai. Būtent dėl šių priežasčių 2018 metais JAV Komercijos departamento Nacionalinių standartų ir technologijų institutas (*angl. U.S. Commerce Department's National Institute of Standards and Technology (NIST)*) (toliau – NIST) pateikė visuomenei atnaujintą 2014 metais sukurtą kritinės infrastruktūros kibernetinio saugumo valdymo modelį (*angl. Framework for Improving Critical Infrastructure Cybersecurity*) (NIST, 2018).

Šiame kibernetinio saugumo valdymo modelyje didžiausias dėmesys skiriamas privataus sektoriaus kibernetinio saugumo valdymo metodų panaudojimui, siekiant sukurti kibernetinėms grėsmėms atsparią organizaciją. NIST sukurto kibernetinio saugumo valdymo modelio diegimas organizacijoje nėra privalomas, bet jo įdiegimas

suteikia kritinių informacinių išteklių valdytojams galimybę identifikuoti, įvertinti ir valdyti kibernetines grėsmes, pasinaudojant prioritetais pagrįsta, lanksčia ir ekonomiškai naudinga metodika (CEA, 2014).

NIST kibernetinio saugumo valdymo modelis yra sudarytas iš 3 sričių, kurių pagrindinis tikslas yra nusakyti ir užtikrinti organizacijos vykdomų funkcijų ir vidaus procesų sąsają su kibernetinio saugumo valdymu organizacijoje:

1. *Kibernetinio saugumo modelio branduolys* – tam tikras veiklų rinkinys, grindžiamas pasauliniais standartais, metodikomis ir praktikomis, suteikiantis galimybę ištransliuoti vidiniais organizacijos komunikacijos kanalais visiems organizacijos nariams suprantamą informaciją apie kibernetinio saugumo veiklą ir rezultatus visoje organizacijoje, į šį procesą įtraukiant kiekvieną organizacijos narį: nuo strateginio iki įgyvendinančiojo lygmens. Modelio branduolys yra sudarytas iš penkių tęstinių funkcijų, kurių sujungimas į vieną bendrą procesą kuria kibernetinio saugumo valdymo organizacijoje dimensiją, nusakančią strateginį požiūrį į kibernetinio saugumo gyvavimo ciklą organizacijoje (NIST, 2018; US-CERT, 2018). Pažymėtina, kad kiekviena kibernetinio saugumo modelio branduolio funkcija identifikuoja tik jai vienai būdingas kategorijas ir veiklas, kurios kuriamos, atsižvelgiant į pasaulinius standartus bei praktikas. NIST kibernetinio saugumo modelio branduolys (žr. 3 paveikslą) sujungia šias funkcijas (NIST, 2018):

- *Identifikavimas* (*angl. identify*) – suteikia organizacijai galimybę nustatyti kibernetines grėsmes, kylančias organizacijos valdomoms sistemoms, žmogiškiesiems ištekliams, turtui, duomenims ir kt.; identifikuoti organizacijos pajėgumus, susijusius su kibernetinio saugumo valdymu. Ši funkcinė sritis nagrinėja išteklių valdymą, verslo aplinką, organizacijos valdymą, narių atsakomybę, rizikų vertinimą, rizikų valdymo strategiją, organizacijos naudojamus išorinius resursus bei paslaugas ir kt.;
- *Apsauga* (*angl. protect*) – sukuriamos ir įgyvendinamos apsaugos priemonės, užtikrinančios kritinių paslaugų teikimą. Šios funkcijos įgyvendinimo priemonės palaiko organizacijos gebėjimą neleisti įvykti kibernetiniam incidentui, o jam įvykus, sumažinti kibernetinio saugumo incidento padarinius. Ši funkcinė sritis nagrinėja vartotojų prieigos prie informacinių išteklių, personalo informavimo ir kibernetinio saugumo mokymo, techninės ir programinės įrangos saugumo, duomenų ir ryšio kanalų saugumo, informacijos apsaugos procedūrų, techninės priežiūros ir naudojamų apsaugos technologijų aspektus;
- *Aptikimas* (*angl. detect*) – apsaugos priemonių, skirtų kibernetiniams saugumo incidentams aptikti, sukūrimas ir naudojimas. Ši funkcinė sritis nagrinėja organizacijoje vykstančių procesų anomalijų stebėjimą ir analizę, nuolatinį kibernetinio saugumo situacijos stebėjimą technologinėje įrangoje, naudojamų apsaugos priemonių efektyvumo vertinimą, aprašo kibernetinių grėsmių ir kibernetinių incidentų aptikimo procesus;
- *Atsakas* (*angl. respond*) – organizacijos galimybės ir gebėjimai tinkamai valdyti aptiktus kibernetinio saugumo pažeidžiamumus, mažinti vykstančių kibernetinio saugumo incidentų padarinius. Šioje kibernetinio saugumo branduolio

srityje nagrinėjamas atsako į kibernetines grėsmes planai, organizacijos komunikavimo planai kibernetinio incidento metu, kibernetinio incidento poveikio organizacijai analizė, kibernetinio saugumo incidento lokalizavimo ir padarinių mažinimo priemonės, įvykusių kibernetinių incidentų analizė ir *išmoktų pamokų* įtraukimas į organizacijos kibernetinio saugumo valdymo strategiją;

- *Atstatymas* (*angl. recover*) – organizacijos veikla, siekiant atstatyti bet kokius pajėgumus ar paslaugas, kurios buvo pažeistos dėl kibernetinio saugumo incidento. Ši sritis nagrinėja organizacijos veiklą ir joje vykstančius procesus, įvykus incidentui.

Šaltinis: *NIST, 2018*

3 paveikslas. *NIST kibernetinio saugumo valdymo modelio branduolys*

2. *Kibernetinio saugumo valdymo pakopos* – organizacijos požiūrio į kibernetinio saugumo valdymą vertinimas, nurodantis, kaip organizacija suvokia kibernetinio saugumo procesus ir šių procesų valdymo riziką. Valdymo pakopos apibūdina kibernetinio saugumo valdymo lygį organizacijoje (nuo pradinio (1 pakopa) iki adaptacinio (4 pakopa)), vertinant jos viduje vykstančių kibernetinio saugumo valdymo procesų charakteristikas bei atsparumo grėsmėms lygį. Siekiant išgryninti organizacijos priklausomybę tam tikrai pakopai, būtina įvertinti tuometinę organizacijos situaciją, susijusią su: rizikos valdymo praktika, grėsmių aplinka, teisinio reguliavimo reikalavimais, organizacijos tikslais, organizaciniais apribojimais ir kt. NIST kibernetinio saugumo pakopai nustatyti yra naudojami trys požymiai: rizikos valdymo procesas; rizikos valdymo programa ir organizacijos dalyvavimas kibernetinio saugumo užtikrinimo ekosistemoje (NIST, 2018). Detalesnis pakopų aprašymas yra pateikiamas toliau:

1 pakopa (pradinė) – rizikų valdymo procesas nėra aiškiai dokumentuotas ir aprašytas, o veiksmai, užtikrinant kibernetinį saugumą organizacijoje, nėra aiškiai suvokiami organizacijos narių; rizikos valdymo programa organizacijoje įgyvendinama spontaniškai; organizacija nebendradarbiauja kibernetinio saugumo klausimais su kitomis organizacijomis;

2 pakopa (informacinė) – rizikų valdymo procesas yra patvirtintas organizacijos vidiniais teisės aktais, bet nėra visiškai įdiegtas; organizaciniu lygmeniu yra žinoma apie kibernetinio saugumo riziką, tačiau rizikos valdymo programa nėra įgyvendinta, o informacija apie kibernetinio saugumo grėsmes yra platinama neformaliais kanalais; organizacijos supratimas apie bendradarbiavimą su kitomis organizacijomis apsiriboja tik kibernetinio saugumo vertinimo ataskaitų parengimu, tačiau pagaminti produktai neviešinami;

3 pakopa (integruota) – rizikų valdymo procesas yra aiškiai dokumentuotas ir organizacijoje naudojamas kasdienei veiklai užtikrinti, o proceso korekcijos atliekamos, atsižvelgiant į organizacijos siekiamus tikslus; rizikos valdymo programa yra suprantama visos organizacijos narių, o reikalui esant, ji yra koreguojama ir atnaujinama; organizacija suvokia save kaip bendros kibernetinio saugumo ekosistemos dalį ir rūpinasi savo teikiamų ir iš išorės gaunamų paslaugų saugumu;

4 pakopa (adaptyvi) – rizikų valdymo procesas organizacijoje yra pagrindžiamas organizacijos patirtimi ir dabartiniu valdymo procesu, tai leidžia organizacijai laiku ir efektyviai reaguoti į kibernetines grėsmes ir prisitaikyti; organizacijos kibernetinio saugumo valdymo programa yra visiškai suderinta su organizacijos verslo procesais ir siekiais, o kibernetinio saugumo situacijos stebėjimas bei kibernetinio saugumo planavimas organizacijoje yra toks pat svarbus, kaip ir finansinių grėsmių vertinimas; organizacija dalyvauja kibernetinio saugumo ekosistemos veikloje, peržiūrėdama, gamindama ir dalindamasi kibernetinio saugumo įžvalgomis su kitais ekosistemos nariais.

3. *Kibernetinio saugumo valdymo profilis* – funkcinių modelio branduolio sričių kategorijų ir subkategorijų rinkinys, suteikiantis organizacijai galimybę suderinti kibernetinio saugumo valdymo procesą su verslo reikalavimais, rizikos tolerancija ir organizacijos ištekliais. Profilis leidžia organizacijai sukurti kibernetinio saugumo rizikų ir pažeidžiamumų valdymo (mažinimo) planą, kuris yra suderintas su organizacijos ir sektoriaus tikslais, teisiniais ir reguliavimo reikalavimais, geriausiomis verslo praktikomis bei atspindi rizikos valdymo prioritetus organizacijoje. Pažymėtina, kad, nagrinėjant kibernetinio saugumo valdymą didelių organizacijų kontekste, galimas kelių, tarpusavyje suderintų profilių naudojimas, atsižvelgiant į tam tikras prioritetines organizacijos veiklos sritis, tačiau organizacijos kibernetinio saugumo valdymo išsivystymas (pakopos nustatymas) bus siejamas su žemiausia konkrečios srities pasiekta kibernetinio saugumo valdymo pakopa (NIST, 2018).

NIST kibernetinio saugumo valdymo modelio įdiegimas organizacijose (kaip ir kitų modelių) nėra privalomas, bet organizacijos ir kritinės infrastruktūros valdytojai gali savarankiškai įdiegti šį modelį savo veiklos procesuose. Atkreiptinas dėmesys, kad šio modelio branduolys yra tam tikras veiklos tęstinumo užtikrinimo ciklas, kurio

vykdymas turi tapti įprasta organizacijos kasdiene veikla. Organizacija, siekdama įdiegti kibernetinio saugumo valdymo procesą, dar prieš jo įdiegimą gali nuspręsti, koks kibernetinio saugumo lygis (pakopa) turi būti pasiektas, ir, atsižvelgdama į turimus išteklius ir priimtą sprendimą, sudaryti kibernetinio saugumo įgyvendinimo planą. Vėliau tikslai gali būti koreguojami, atsižvelgiant į organizacijos prioritetus ir aplinkos situaciją.

Atkreiptinas dėmesys, kad NIST modelyje kibernetinis saugumas yra nagrinėjamas ne tik technologiniu aspektu. Modelyje vertinamas ir žmogiškasis faktorius, organizaciją supanti aplinka, o pati organizacija yra traktuojama kaip ekosistemos dalis, kuri turi prisidėti prie bendro visos ekosistemos kibernetinio saugumo gerinimo.

1.3.3. (ISC)² kibernetinio saugumo valdymo modelis

Tarptautinis informacinių sistemų saugumo sertifikavimo konsorciumas (angl. *International Information Systems Security Certification Consortium (ISC)²*) sukūrė sertifikuotų informacinių sistemų saugumo profesionalų (*angl. Certified Information Systems Security Professionals (CISSP)*) mokymo programą, kuri dabartiniu laikotarpiu yra viena iš labiausiai paplitusių kibernetinio saugumo specialistų ruošimo ir sertifikavimo programų. Šios kibernetinio saugumo specialistų mokymo programos panaudojimas organizacijoje yra vienas iš būdų įdiegti kibernetinio saugumo valdymo modelį, kuris būtų suderintas su (ISC)² aprašytomis kibernetinio saugumo funkcinėmis sritimis (Donaldson ir kt., 2015). (ISC)² kibernetinio saugumo valdymo modelis yra sudarytas iš aštuonių kibernetinio saugumo domenų:

- *Saugumo ir rizikų valdymo domenas* yra susijęs su organizacijos procesais, politika, koncepcijomis, principais, struktūromis ir standartais, naudojamais organizacijos informaciniams ištekliams apsaugoti, taip pat, šių apsaugos priemonių veiksmingumui organizacijos valdymo, organizacijos elgesio ir kibernetinių grėsmių suvokimo srityse įvertinti. Saugumo ir rizikų valdymas leidžia organizacijai sukurti kibernetinio saugumo valdymo programą, apimančią administracines, technines ir fizines saugumo užtikrinimo priemones, kurios yra būtinos, norint užtikrinti informacinių išteklių konfidencialumą, vientisumą ir prieinamumą. Tinkamai įgyvendinusi kibernetinio saugumo valdymo programą, organizacija užsitikrins naudojamų informacinių išteklių veikimą bei pačios organizacijos veiklos tęstinumą. Šiame domene nagrinėjami teisiniai, organizacijos valdymo ir rizikos valdymo atitikimo, saugumo valdymo organizacijoje ir kiti aspektai;
- *Išteklių saugumas* apibrėžia sąvokas, principus, struktūras ir standartus, kurie yra naudojami organizacijos valdomiems ištekliams stebėti ir apsaugai, siekiant užtikrinti turimų išteklių konfidencialumą, vientisumą ir pasiekiamumą. Šis kibernetinio saugumo valdymo modelio domenas aprašo organizacijos kibernetinio saugumo architektūrą, nustatant kibernetinio saugumo priemonių panaudojimo organizacijoje planą, kuris, jį įgyvendinus, užtikrins organizacijos valdomų išteklių (saugumo procesų, apsaugos sistemų ir kt.) saugumą bei sudarys sąlygas maksimaliai suderinti kibernetinio saugumo valdymą su organizacijos siekiamais tikslais ir strategine kryptimi;

- *Architektūros domenas* nagrinėja kibernetinio saugumo architektūros principus ir standartus, naudojamus projektuojant, diegiant, stebint ir saugant operacines sistemas, techninę ir programinę organizacijos valdomų išteklių dalį. Šiame saugumo domene atkreipiamas dėmesys į informacinių sistemų saugumo vertinimą, technologinės architektūros saugumo pažeidžiamumus, programinės įrangos saugumo pažeidžiamumus, kriptografinių priemonių naudojimo aspektus ir technologines saugumo priemones, skirtas fiziniam patalpų, kuriose apdorojama organizacijos valdoma informacija, saugumui užtikrinti;
- *Telekomunikacinių tinklų saugumo domenas* nagrinėja struktūras, duomenų perdavimo technologijas ir formatus bei kitas saugumo priemones, naudojamas duomenų konfidencialumui, vientisumui ir prieinamumui užtikrinti, perduodant jas per privačius ir viešuosius ryšių tinklus. Telekomunikacinių tinklų saugumas dažniausiai suprantamas kaip informacinių technologijų saugumo pagrindas ir laikomas vienu svarbiausiu, jei ne pats svarbiausias, organizacijos valdomu informaciniu ištekliu. Telekomunikacinio tinklo saugumo pažeidimas (konfidencialumo, vientisumo, prieinamumo, autentiškumo ar gyvybingumo savybės pažeidimas) bet kokiame lygmenyje gali turėti pražūtingų pasekmių, o visapusiška telekomunikacinio tinklo kontrolė suteikia galimybę lengvai ir nuosekliai lokalizuoti vykstančią arba numatyti gresiančią kibernetinę ataką;
- *Prieigos valdymo ir tapatybės nustatymo domenas* yra turbūt dažniausiai sutinkamas saugumo aspektas, nagrinėjamas kibernetinio saugumo valdymo modeliuose. Prieigos kontrolė apima visus organizacijos veiklos lygius: *infrastruktūra* – prieigos kontrolė apsaugo organizaciją nuo neteisėto piktavalių patekimo į organizacijos fizines buveines, siekiant apsaugoti viduje esantį personalą, įrangą, informaciją ir kitus išteklius; *informacinės sistemos* – daugiapakopė prieigos kontrolės sistema yra laikoma šiuolaikinių informacinių sistemų standartu, o jos panaudojimas apsaugo šias sistemas ir jų apdorojamą, saugomą ar perduodamą informaciją nuo žalos ar piktnaudžiavimo; *personalas* – organizacijos nariai, klientai, verslo partneriai ir visi kiti asmenys, susiję su organizacija, turi būti kontroliuojami, kad būtų užtikrinta efektyvi suinteresuotų asmenų sąveika. Informacijos saugumo pagrindinis tikslas yra užtikrinti organizacijos valdomų informacinių išteklių pasiekiamumą, tuo pačiu metu užtikrinant CIA triados principus, apimant tiek fizinį organizacijos turtą (pastatus, įrangą, žmones), tiek informacinius išteklius (informaciją, duomenis, informacines sistemas). Prieigos kontrolė atlieka pagrindinį vaidmenį, užtikrinant sistemų ir informacijos konfidencialumą. Prieigos prie fizinio ir informacinio organizacijos turto valdymas yra labai svarbus, siekiant sumažinti grėsmes ir užkirsti kelią nesankcionuotam duomenų panaudojimui, o šiam tikslui pasiekti yra būtini aiškūs nuostatai, nusakantys, kas gali matyti, naudoti, keisti ar naikinti organizacijos valdomą turtą. Pažymėtina, kad prieigos valdymas užtikrina, kad vertingi organizacijos duomenys ir kritinės paslaugos nebus piktybiškai paveikti piktavalių, pasisavinti ar pavogti;
- *Saugumo vertinimas ir testavimas* nusako periodinio kibernetinio saugumo vertinimo ir pažeidžiamumų testavimo metodų, technikų ir standartų panaudojimą,

siekiant identifikuoti esamus kibernetinio saugumo sistemos trūkumus, taip pat apsisaugoti nuo galimų, dar nežinomų saugumo pažeidžiamumų. Pagrindinis šiame domene aptariamų saugumo vertinimų ir testavimų tikslas yra suteikti organizacijai ir jos nariams žinių, padėsiančių valdyti rizikas ir grėsmes, susijusias su informacinių sistemų kūrimu, veikimu ir palaikymu. Naudodamasi periodiniais sistemų kibernetinio saugumo vertinimais ir testavimais bei analizuodama šių vertinimų išvadas, organizacija gali numatyti priemones, kurios gali pagerinti ir užtikrinti naudojamų sistemų apsaugos galimybes, nusakyti apribojimus, gerinti ir optimizuoti organizacijos veiklos procesuose naudojamas sistemas. Pažymėtina, kad saugumo vertinimo ir testavimo priemonės turi būti naudojamos visuose informacinių sistemų gyvavimo ciklo etapuose, kad kuo anksčiau būtų sužinoma apie planuojamų (arba jau diegiamų) sistemų stipriąsias ir silpnąsias puses. Tikslingiausias yra ankstyvas techninių ir operacinių sistemos trūkumų nustatymas, kadangi šie veiksmai užtikrina sklandų tolimesnių darbų vykdymą. Saugumo vertinimo ir testavimo procesas apima: planavimą technologijų plėtrai, įskaitant galimas plėtros rizikas; sistemos architektūrinės dalies vertinimą, atsižvelgiant į sistemos misiją; sistemų prototipų vertinimą ir kt.;

- *Saugumo užtikrinimo domenas* – apibrėžia priemones, standartus ir metodus, naudojamus siekiant identifikuoti organizacijos kritinius išteklius (infrastruktūrą, informaciją, procesus ir kt.) ir užkirsti galimybę nesankcionuotam šių išteklių panaudojimui arba sumažinti šių išteklių pažeidžiamumą. Šiems tikslams naudojamos auditavimo ir stebėjimo priemonės, įrankiai ir mechanizmai leidžia nustatyti įvykusius kibernetinio saugumo incidentus, jų atsiradimo priežastis ir pasekmes bei pateikti incidentą nagrinėjantiems asmenims išsamią informaciją apie jo eigą ir pasekmes. Kasdienis organizacijos išteklių ir procesų stebėjimas ir priežiūra užtikrina kibernetinio saugumo organizacijoje tvarumą;
- *Programinės įrangos saugumo domeno* nuostatos apibrėžia kibernetinio saugumo veiksmus, susijusius su programinės įrangos naudojimu organizacijos veiklai užtikrinti: būtinas kibernetinio saugumo valdymas programinės įrangos gyvavimo ciklo metu; kibernetinio saugumo užtikrinimo nuostatos turi būti taikomos visoms organizacijos sistemoms, nepaisant tų sistemų statuso (diegiama, naudojama, bandoma); būtinas periodinis saugumo testavimas visai programinei įrangai, naudojamai organizacijos veikloje, siekiant nustatyti programinės įrangos saugumo efektyvumą; būtinas įsigyjamos programinės įrangos saugumo vertinimas, kuris atliekamas prieš įsigijimo procesą. Pažymėtina, kad nors kibernetinis saugumas tradiciškai pabrėžia prieigos prie informacinių sistemų kontrolės funkcijas, saugumo specialistas privalo užtikrinti, kad organizacijos savo saugumą orientuotų ir į programinę įrangą, kadangi didžioji dalis kibernetinio saugumo incidentų viena ar kita forma pasireiškia per programinės įrangos pažeidžiamumus, o šie pažeidžiamumai neretai tampa savotiškais „vartais“ į organizacijos vidines sistemas.

Apibendrinant galima pažymėti, kad (ICS)[2] kibernetinio saugumo valdymo modelis kibernetinį saugumą daugiausiai nagrinėja technologijų įgyvendinimo ir naudoji-

mo kontekste. Šiame modelyje menkai aptariamos organizacijos narių (darbuotojų) ir organizacijos partnerių (paslaugų ir įrangos tiekėjų) edukacijos, tobulinimo ir kibernetinio saugumo valdymo kultūros tarporganizaciniu lygiu klausimai. Pažymėtina, kad modelyje nėra nagrinėjami organizacijai būtini išorinės aplinkos stebėjimo veiksmai (apsiribojama tik vidinės organizacijos aplinkos stebėjimu), suteikiantys galimybę numatyti kibernetinio saugumo pažeidžiamumų atsiradimą, taip pat nėra aptariama organizacijos rolė ir jos dalyvavimas globalioje kibernetinio saugumo ekosistemoje.

1.3.4. ISO27001/27002 kibernetinio saugumo valdymo priemonės

Tarptautinis ISO27001/27002 standartas yra skirtas organizacijoms ir sudarytas kaip rekomendacinių priemonių rinkinys, kurio paskirtis užtikrinti organizacijos išteklių valdymą bei įgyvendinti visuotinai pripažintas informacijos saugumo valdymo priemones. Šio standarto naudojimas organizacijoje yra savanoriškas, bet jis gali užtikrinti kibernetinio saugumo ir informacijos valdymą organizacijoje, kuri renka, apdoroja, saugo ir perduoda informaciją įvairiomis formomis, įskaitant elektroninę, fizinę ir žodinę. Pažymėtina, kad informacijos sąvoka ISO27001/27002 standarte yra apibrėžiama platesniu aspektu nei rašytiniai žodžiai, skaičiai ir vaizdai. ISO27001/27002 apibūdina informaciją taip: žinios, koncepcijos, idėjos ir prekių ženklai taip pat yra nematerialios informacijos formos. Atkreiptinas dėmesys, kad šiuolaikiniame ryšių ir informacinių technologijų pasaulyje informacija, valdymo procesai, sistemos, ryšių tinklai ir personalas, dalyvaujantis organizacijos veikloje, yra turtas, kuris privalomai turi būti apsaugotas nuo įvairių jam kylančių pavojų (LSD, 2014).

Pažymėtina, kad ISO27001/27002 standarto kūrėjai mano, jog vienintelė galimybė tinkamai įgyvendinti saugumą yra pasiekiama, įgyvendinant tinkamą valdymo priemonių (organizacinių struktūrų bei techninės ir programinės įrangos funkcijų) rinkinį, kuris nusako, kokios *valdymo priemonės turi būti numatytos, įgyvendintos, stebimos, peržiūrimos ir, prireikus, gerinamos, siekiant užtikrinti, kad būtų pasiekti konkretūs organizacijos saugumo ir veiklos tikslai*. Atkreiptinas dėmesys, kad pagal ISO27001/27002, kibernetinis saugumas organizacijoje traktuojamas kaip technologinis saugumo įgyvendinimo procesas, kuris gali būti pasiekiamas tam tikromis technologinėmis priemonėmis. Tačiau pažymėtina, kad vien tik technologinių saugumo užtikrinimo priemonių naudojimas yra nepakankamas, todėl kibernetinio saugumo įgyvendinimas organizacijoje turėtų būti grindžiamas atitinkamu valdymo procesų ir procedūrų panaudojimu, atidžiu planavimu ir esamos situacijos stebėjimu. Norint sukurti sėkmingai ir efektyviai veikiančią kibernetinio saugumo valdymo sistemą (modelį), yra būtinas visų suinteresuotų organizacijos narių palaikymas ir adekvatus kibernetinio saugumo situacijos suvokimas visos organizacijos mastu, kadangi būtent tai gali garantuoti kritinių išteklių saugumą ir organizacijos veiklos procesų tęstinumą.

Pagal ISO27001/27002 standartą pirminis kibernetinio saugumo valdymo įgyvendinimo organizacijoje žingsnis yra siejamas su būtinybe organizacijai nustatyti saugumo reikalavimų kriterijus. Saugumo reikalavimų kriterijų nustatymas yra siejamas su trimis sritimis, kurios apsprendžia kibernetinių grėsmių atsiradimą (LSD, 2014):

1. rizikų, susijusių su organizacijos veikla, vertinimas, kuris analizuoja bendrą visos organizacijos veiklos strategiją ir organizacijos siekiamus tikslus. Atliekant rizikos vertinimą, nustatomos grėsmės organizacijos valdomiems ištekliams, įvertinamas galimas išteklių pažeidžiamumas grėsmių atsiradimo atveju, grėsmių atsiradimo tikimybė bei apskaičiuojamas galimas grėsmių poveikis;
2. teisiniai, reguliavimo ir kiti sutartiniai reikalavimai, kurių organizacija ir jos nariai privalo laikytis, bei organizacijos narių socialinė ir kultūrinė aplinka;
3. informacinių išteklių panaudojimo reikalavimų rinkinys, kuris yra būtinas organizacijos veiklos tęstinumui ir stabilumui užtikrinti.

Įgyvendinant kibernetinio saugumo valdymo priemones organizacijoje, organizacijos panaudojami ištekliai turi būti suderinami su galima žala organizacijos veiklai, kuri galėtų atsirasti dėl saugumo pažeidžiamumų sąlygotų incidentų, jei nebūtų naudojamos numatomos kibernetinio saugumo valdymo priemonės. Rizikos vertinimo procesas ir gauti rezultatai užtikrina sėkmingą organizacijos kibernetinio saugumo situacijos valdymą, nustato būtinus valdymo veiksmus ir prioritetus, įgyvendinant organizacijos atsparumo kibernetiniams incidentams tikslus.

ISO27001/27002 standartas numato keturiolika saugumo valdymo sričių, kuriose yra apibrėžiamos tam tikros saugumo valdymo priemonės, kurių panaudojimas kiekvienoje organizacijoje yra siejamas tik su konkrečios organizacijos veiklos procesais. Organizacija, įgyvendindama kibernetinio saugumo valdymą, atsižvelgdama į aplinkybes, pati nustato, kurių sričių saugumo valdymo priemonės turi būti naudojamos ir kokia yra naudojamų priemonių svarba organizacija. Būtent dėl šios priežasties kiekviena ISO27001/27002 standartą taikanti organizacija turėtų nustatyti tik jai tinkamas kibernetinio saugumo valdymo priemones, jų svarbą ir jų taikymą atskiriems verslo procesams (LSD, 2014). Pažymėtina, kad toliau išvardytos saugumo sritys nėra įvardinamos prioriteto tvarka:

- *informacijos saugumo politikos* sritis: informacijos saugumo valdymo gairės, apibrėžiančios organizacijos požiūrį į kibernetinio saugumo užtikrinimo tikslus organizacijoje. Tikslai turi būti nustatyti organizacijos vadovybės, patvirtinti ir perduoti susipažinti organizacijos nariams, taip pat kitoms organizacijoms, dalyvaujančioms organizacijoje vykstančiose vidaus valdymo procesuose. Taip pat turi būti numatytas periodiškas informacijos saugumo politikos vertinimas ir, esant būtinumui, koregavimas, siekiant užtikrinti jos tinkamumą, adekvatumą ir veiksmingumą. Pažymėtina, kad organizacijos saugumo valdymo gairės privalo atitikti galiojančias teisės normas;
- *informacijos saugumo organizavimo* sritis, nagrinėjanti kibernetinio saugumo įgyvendinimo, naudojimo ir kontrolės sistemas organizacijoje bei mobilių technologinių įrenginių ir nuotolinio darbo panaudojimą organizacijos veikloje. Šioje srityje apibrėžiamos technologinės ir organizacinės kibernetinio saugumo priemonės, organizacijos narių atsakomybių ribos, pažeidžiamumai ir grėsmės organizacijos veiklos procesams;
- žmogiškųjų išteklių saugumo sritis, kurios tikslas užtikrinti organizacijos narių ir kitų su organizacija susijusių asmenų atsakomybės suvokimą, dirbant organi-

zacijoje, vykdant organizacijos vadovybės pavestas užduotis, bendradarbiaujant su organizacija, taip pat saugant konfidencialią informaciją, kuri buvo patikėta subjektams, dalyvaujantiems organizacijos veiklos procesuose;

- *išteklių valdymo* saugumo sritis apima materialaus ir nematerialaus (informacija, duomenys) organizacijos turto naudojimo reglamentavimą, kuris yra būtinas, siekiant tinkamai valdyti organizacijos turimus išteklius bei apsaugoti juos nuo tyčinio ar netyčinio praradimo ir / ar sunaikinimo;
- *prieigos prie techninės įrangos valdymo* sritis, reglamentuojanti organizacijos narių veiklą ir informacijos saugumo reikalavimus, siekiant apsaugoti organizacijos išteklius nuo neteisėtos fizinės prieigos ir neteisėto panaudojimo. Organizacija turi nustatyti ir patvirtinti aiškias vidaus taisykles, nusakančias, kokia techninė įranga gali būti naudojama konkrečių organizacijos narių ir kokiomis sąlygomis (konfigūravimo pakeitimų registravimas, pakeitimus vykdančių asmenų nustatymas ir kt.);
- *vartotojų identifikavimo ir prieigos valdymo* sritis apibrėžia organizacijos narių prieigą prie programinės įrangos, sistemų ir kitų išteklių bei jų teikiamų paslaugų reikalavimus; naudotojų atsakomybę; prieigos duomenų tvarkymą;
- *kriptografinių priemonių* naudojimas nustato tinkamą ir veiksmingą kriptografinių priemonių ir mechanizmų panaudojimą, siekiant apsaugoti informacijos konfidencialumą, autentiškumą bei vientisumą;
- *fizinio saugumo* sritis reglamentuoja fizinį organizacijos saugumą, įeigos kontrolės bei priežiūros mechanizmus, naudojamos technologinės įrangos fizinės apsaugos priemones, energetinio saugumo organizacijoje klausimus;
- *darbo saugos sritis,* nustatanti: procedūras, taikomas eksploatavimo veiklai, susijusiai su informacijos apdorojimo ir ryšių priemonėmis (kompiuterių įjungimo ir išjungimo procedūromis, duomenų atsarginių kopijų darymu, įrangos techninę priežiūra, duomenų laikmenų priežiūra, kompiuterių patalpų ir pašto naudojimo valdymu ir saugumu); pakeitimų valdymą; įrangos našumo analizę; kūrimo ir testavimo procedūras; apsaugos nuo piktybinės programinės įrangos užtikrinimo mechanizmus; techninės ir programinės įrangos gedimus ir anomalijas; programinės įrangos ir galimų pažeidžiamumų valdymą organizacijoje;
- *telekomunikacijų saugumo* sritis reglamentuoja ryšio technologijų ir tinklų naudojimą; organizacijos tinklų fizinio ar loginio atskyrimo procedūras; perduodamos informacijos saugumo reikalavimus ir kt.;
- *informacinių sistemų gyvavimo ciklo saugumo* sritis numato priemones, užtikrinančias, kad informacijos saugumas būtų integrali visų organizacijos veiklos procesuose naudojamų informacinių sistemų dalis per visą jų gyvavimo ciklą;
- *santykių su tiekėjais saugumo valdymas* nagrinėja taisykles ir reikalavimus, užtikrinančius organizacijos išteklių, prieinamų tiekėjams, apsaugą;
- *kibernetinių saugumo incidentų valdymas* apibrėžia incidentų, įskaitant komunikavimo dėl saugumo įvykių procesus valdymą, akcentuojant šios veiklos nuoseklumą ir efektyvumą;
- *organizacijos kibernetinio saugumo veiklos tęstinumo valdymo* sritis nagrinėja organizacijos gebėjimus valdyti kibernetinį saugumą kaip vieną iš kasdienių

organizacijos procesų, pasirengiant kibernetinio saugumo planavimui ir įgyvendinimui taip, kad, įvykus kibernetiniam incidentui, organizacijos veikla nebūtų veikiama incidento padarinių.

Apibendrinant ISO27001/27002 kibernetinio saugumo valdymo modelį, galima teigti, kad jame pagrindinis dėmesys yra atkreipiamas į organizacines kibernetinio saugumo užtikrinimo priemones, kurios apibrėžiamos kaip tam tikrų reglamentuojančių vidinių teisės aktų ir taisyklių parengimu bei jų naudojimu organizacijos vidaus procesuose. Šis kibernetinio saugumo valdymo modelis, kaip ir kiti, anksčiau aptarti kibernetinio saugumo valdymo modeliai, nagrinėja ir technologines priemones, kurios užtikrina fizinės prieigos prie technologinių įrenginių aspektus, ryšio tinklų, programinės įrangos, kitų informacinių išteklių naudojimo stebėjimo sistemas, tačiau ISO27001/27002 standartas nenagrinėja personalo saugumo klausimus, susijusius su organizacijos narių mokymu ir informavimu apie kibernetinius incidentus, rizikų ir pažeidžiamumų atpažinimu. Pažymėtina, kad šis kibernetinio saugumo valdymo modelis nenagrinėja pačios organizacijos kaip kibernetinio saugumo ekosistemos dalies, kurioje kiekvienas ekosistemos narys sugeba rinkti ir sisteminti informaciją apie savo vidaus kibernetinio saugumo situaciją bei, dalindamasis šia informacija su kitais nariais, prisidėti prie globalaus kibernetinio saugumo situacijos gerinimo. Šis kibernetinio saugumo valdymo modelis koncentruojasi į standartinį *Planuok-Daryk-Tikrink-Veik* (*angl. Plan-Do-Check-Act*) kibernetinio saugumo veiklos vykdymo užtikrinimo ciklą (Donaldson ir kt., 2015), kuris yra labiau tinkamas nedidelėms statinėms organizacijoms, kurios nedalyvauja globaliose kibernetinio saugumo ekosistemose.

1.3.5. Kibernetinio saugumo valdymo modelių lyginamoji analizė

Apibendrinant visus nagrinėtus kibernetinio saugumo valdymo modelius, galima teigti, kad visi anksčiau aprašyti kibernetinio saugumo modeliai yra skirti kibernetiniam saugumui užtikrinti bet kokio sektoriaus ar veiklos organizacijoje: valstybinis sektorius, viešojo ar privataus verslo atstovai, gynybinės organizacijos ir kt., o pačias modeliuose aptariamas saugumo priemones galima išskirstyti į tris sritis: fizines saugos, technologinės saugos ir administracinės saugos priemones.

Kiekvieno iš anksčiau aptartų (taip pat ir kitų, šiame disertaciniame darbe nepaminėtų) kibernetinio saugumo valdymo modelių taikymas organizacijoje yra savanoriškas ir grindžiamas tik pačios organizacijos ir jos narių kibernetinio saugumo būtinybės suvokimu. Pažymėtina, kad šis organizacinis suvokimas yra būdingas tik toms organizacijoms, kurios savo kasdieniuose veiklos procesuose naudoja sudėtingas ryšių ir informacinių technologijų sistemas, veikia globalioje aplinkoje, pasižymi didele teritorine sklaida arba didelių organizacijos narių skaičiumi. Pasak S. Beissel, šiuolaikinis globalus pasaulis, informacinės ir telekomunikacinės technologijos, kibernetinio saugumo grėsmės ir kiti faktoriai diktuoja organizacijoms kibernetinio saugumo valdymo būtinybę, bet tik išsivysčiusi organizacija, sugebanti įvertinti naujų technologijų keliamas grėsmes, apskaičiuoti galimų grėsmių riziką, numatyti kibernetinių incidentų padarinius, sugebės efektyviai valdyti savo kibernetinį saugumą (Beissel, 2016).

Fizinės saugos priemonių, aptariamų modeliuose, visuma aptaria saugumo organizavimo klausimus, susijusius su patekimu ir judėjimu organizacijos buveinėse, organizacijos valdomų išteklių naudojimo apribojimais ir kt., ir faktiškai apima visą saugumo priemonių spektrą.

Aprašant organizacinės saugos priemonės nagrinėtuose modeliuose, būtina akcentuoti, kad kiekviename modelyje ypatingas dėmesys yra atkreipiamas į būtinybę parengti ir patvirtinti organizacijos vidaus tvarkas ir taisykles, kurios turi atitikti galiojantį teisinį reglamentavimą bei derėti su organizacijos siekiamais tikslais ir strategija.

Lyginant visus anksčiau nagrinėtus kibernetinio saugumo valdymo modelius, galima pažymėti, kad jų sandara daugiausiai yra orientuota į technologinę kibernetinio saugumo valdymo dimensiją, nors patys siūlomi kibernetinio saugumo valdymo modeliai ir yra technologiškai neutralūs. Modeliuose akcentuojamos tam tikros kibernetinio saugumo užtikrinimo (informacijos saugos valdymo) priemonės, kurios šiuolaikiniame, informacinėmis technologijomis grįstame pasaulyje yra tapusios kibernetinio saugumo postulatais.

Pažymėtina, kad menkiausiai kibernetinio saugumo valdymo modeliuose nagrinėjama sritis yra siejama su personalo valdymu (kibernetinio saugumo kultūros formavimo aspektais). ISO27001/27002 standarto modelyje žmogiškųjų išteklių sritis menkai nagrinėja personalo saugumo klausimus, susijusius su personalo mokymu, informavimu apie kibernetinius incidentus, rizikų ir pažeidžiamumų atpažinimu, tačiau didelis dėmesys yra skirtas grėsmėms kibernetiniam saugumui identifikuoti, vykdant personalo atrankas ir koordinuojant darbą (patikrinimas priimant į pareigas, darbo santykių metų ir nutraukiant darbo santykius). SANS instituto modelyje žmogiškojo faktoriaus svarba akcentuojama žmogiškųjų išteklių valdymo srityje, apimančioje darbuotojų mokymą, personalo atsakomybių nustatymą, kibernetinių incidentų valdymo taisykles, kibernetinio saugumo pratybas (nagrinėjamos organizacijos narių kompetencijos kibernetinių incidentų identifikavimo, lokalizavimo ir valdymo sektoriuose). (ICS)[2] kibernetinio saugumo valdymo modelis menkai aptaria organizacijos narių (darbuotojų) ir organizacijos partnerių (paslaugų ir įrangos tiekėjų) edukaciją, tobulinimą ir kibernetinio saugumo valdymo kultūros klausimus. Pažangiausiu kibernetinio saugumo valdymo modeliu personalo srityje gali būti laikomas NIST modelis, kuriame didelis dėmesys yra skiriamas tiek vidiniams organizacijos nariams mokyti ir informuoti, tiek ir organizacijos narių ir pačios organizacijos ryšiams su išorės aplinka.

Visi nagrinėti kibernetinio saugumo valdymo modeliai ir modeliuose aptariami kibernetinio saugumo įgyvendinimo priemonių realizacijos mechanizmai yra grindžiami veiksmų planavimo ir realizacijos ciklo (*angl. Plan-Do-Check-Act*) nuostatomis, kurios yra būtinos, vykdant bet kokius organizacijos veiklos procesus. Tačiau pažymėtina, kad tik NIST modelis ir šio modelio branduolio struktūra numato ne tik tam tikros kibernetinio saugumo srities organizavimą, vadovaujantis anksčiau minėtu ciklu, bet ir nusako visos kibernetinio saugumo valdymo sistemos organizacijoje veiklą. Vieninteliame (iš nagrinėtų šioje disertacinio darbo dalyje) NIST modelyje yra nustatomi keturi organizacijos brandumo lygiai, kurie skatina organizaciją siekti tam tikro kibernetinio saugumo išsivystymo lygio, kuris nusako organizacijos vietą globalioje

kibernetinio saugumo ekosistemoje. NIST kibernetinio saugumo valdymo modelis yra labiausiai tinkamas, nagrinėjant kibernetinį saugumą, kadangi pagrindinis kibernetinio saugumo iššūkis yra siejamas su nuolat besikeičiančia aplinka, o būtent dėl šios priežasties organizacija turi būti organiška, sugebanti greitai ir efektyviai prisitaikyti prie ją supančios, besikeičiančios aplinkos.

Atlikus anksčiau nagrinėtų kibernetinio saugumo valdymo modelių palyginimą pagal T. Limbos, K. Agafonov ir kitų mokslininkų 2017 metais pasiūlytą kibernetinio saugumo valdymo modelį (Limba ir kt., 2017), kuriame kibernetinis saugumas yra nagrinėjamas šešių dimensijų kontekste, visų disertacijoje apžvelgtų modelių sritis galima pavaizduoti žemiau pateikiamoje lentelėje (žr. 1 lentelę).

1 lentelė. *Kibernetinio saugumo valdymo modelių lyginamoji analizė*

	Organizacijos valdymo priemonės	**Teisinis reguliavimas**	**Kibernetinio saugumo kultūros aspektai**	**Technologinio saugumo valdymas**	**Rizikos valdymas**	**Incidentų valdymas**
SANS modelis			X	X		X
NIST modelis	X		X	X	X	
(ISC)² modelis	X	X		X		
ISO27001/27002 modelis		X		X	X	X

Šaltinis: *sudaryta autoriaus*

Atkreiptinas dėmesys, kad nei vienas iš šiame disertaciniame darbe nagrinėtų ir pasaulyje naudojamų kibernetinio saugumo valdymo modelių kibernetinio saugumo valdymą nevertina visapusiškai per visas įmanomas vertinimo prizmes, tačiau būtent toks kibernetinio saugumo valdymo organizavimas yra labiausiai tinkamas siekiant užtikrinti visapusišką kibernetinį saugumą (Limba ir kt., 2017), kuris yra privalomas įgyvendinant elektroninius rinkimus. Taip pat pažymėtina, kad nors nagrinėtose modeliuose ir yra atlikta tam tikrų kibernetinio saugumo valdymo sričių analizė (pvz. personalo atsakomybių identifikavimas, technologinis saugumas ir kt.), dažnai jos nepilnai apima tam tikrą kibernetinio saugumo valdymo dimensiją bei jos atsakomybes sritis. Akcentuotina, kad siekiant saugių elektroninių rinkimų įgyvendinimo, kibernetinį saugumą reikia nagrinėti žymiai platesniame kontekste, nei tai tradiciškai daro anksčiau apžvelgti valdymo modeliai (pvz. personalo valdymas turi būti nagrinėjamas ne tik išteklių valdymo ar atsakomybių nustatymo aspektais, bet ir mokymo kontekste), kadangi tik toks konceptualus požiūris į kibernetinį saugumą gali užtikrinti saugių rinkimų įgyvendinimą ir praplėsti tradiciškai nagrinėjamų kibernetinio saugumo sričių ribas.

1.4. Kibernetinio saugumo incidentų taksonomija e-rinkimų kontekste

Ši disertacinio darbo dalis bus skirta kibernetinių incidentų taksonomijai elektroninių rinkimų sistemų kontekste sukurti. Šioje disertacinio darbo dalyje nagrinėti mokslininkų darbai suteikią galimybę sukurti elektroninių rinkimų kibernetinio saugumo taksonomiją, išsamiai aprašančią galimus kibernetinio saugumo incidentus elektroninėse balsavimo sistemose ir identifikuojančią galimus kibernetinių incidentų sukėlėjus, jų siekiamus tikslus ir naudojamus kibernetinių atakų metodus.

Kibernetinių incidentų pagrindinis tikslas – paveikti individo ar jų grupės elgesį, sukuriant painiavą ir informacijos perteklių (Cayirci, Ghergherehchi, 2011). Pasaulio mokslininkų atlikti moksliniai tyrimai rodo, kad, nepaisant žiniasklaidoje plačiai aprašomų kibernetinių atakų poveikio visuomenei, organizacijoms ir valstybėms kibernetinis saugumas ir su juo siejamos grėsmės ir rizikos vis dar nėra plačiai analizuojamos bei viešinamos organizacijų vidinėje ir išorinėje aplinkose. Mokslininkai pažymi, kad, nors visuomenėje informavimas apie kibernetinių atakų grėsmes ir jų padarinius ir toliau didėja, nesuskaičiuojamas šių įvykių klasifikavimo metodų skaičius neleidžia techniniams darbuotojams, organizacijų vadovams ir organizacijų veiklos politikos kūrėjams dalyvauti prasmingose diskusijose apie riziką jų atstovaujamose organizacijose. Kibernetinių incidentų kieko pasaulyje augimas paskatino atliekamų mokslinių tyrimų didėjimą akademinėje visuomenėje, tačiau tyrimuose dominuoja technologiniai mokslai ir teisė, o literatūra, susijusi su kibernetinių grėsmių aplinka, dėl savo terminijos specifiškumo dažnai yra nesuprantama plačiam visuomenės sluoksniui ir apsunkina visuomenės kibernetinio saugumo situacijos supratimą. Ši situacija taip pat gali sukelti nesusipratimų tarp technologinių žinių turinčių specialistų ir organizacijų vadovų, o tai ateityje gali sukelti beprasmišką išteklių panaudojimą organizacijose bei sudaryti galimybes organizacijoms patirti didelių finansinių išlaidų. Šiose srityse per paskutinius du dešimtmečius neabejotinai buvo padaryta pažanga, tačiau taip pat turime pripažinti, kad elektroninės grėsmės visada vystosi ir praeities scenarijai gali kartotis (Harrison, White, 2011; Ferdinand, Benham, 2017; Harry, 2018, Chase, 2019).

Kaip jau buvo pažymėta anksčiau, mūsų pasaulis tampa vis labiau tarpusavyje susijęs, nes svarbios viešojo ir privataus sektoriaus paslaugos bei pasaulinė infrastruktūra yra priklausomos nuo skaitmeninės informacijos ir technologijų (Johnson, 2015; Beissel, 2016; Chase, 2019). Taigi, grėsmė konfidencialumui, vientisumui ir skaitmeninio pobūdžio informacijos prieinamumui yra vienas iš svarbiausių aspektų, norint užtikrinti kibernetinį saugumą valstybėse, organizacijose, suteikti apsaugą viešojo ir privataus sektoriaus paslaugų vartotojams. Šviečiant visuomenę, diegiant kibernetinio saugumo kultūrą organizacijose, taip pat naudojantis kibernetinio saugumo incidentų valdymo įgyvendinimo planais, neabejotinai gali būti pagerintas visuotinis kibernetinio saugumo supratimas, taip pat sumažinamas kibernetinių grėsmių plitimo mastas. Taip pat organizacijos, skirdamos papildomą dėmesį savo kibernetinio saugumo vertinimui ir supratimui, gali suteikti sau galimybę pagerinti savo kibernetinį atsparumą, tokiu būdu sumažindamos savo kaštus, siekdamos valdyti kibernetinius incidentus arba atstatyti įprastus organizacijos veiklos procesus po kibernetinio saugumo incidentų (Ferdinand, Benham, 2017).

Siekdami nustatyti tinkamus veiklos procesus organizacijų kibernetiniam saugumui valdyti, pasaulio mokslininkai atliko tyrimus, kurių pagrindinis tikslas buvo sukurti kibernetinių atakų ir incidentų klasifikavimo sistemą. Formaliai kibernetinio saugumo problemų tyrimų pradžia galima laikyti XX amžiaus aštuntąjį dešimtmeti, kai kompiuteriai buvo pradėti naudoti valstybinėse įstaigose ir universitetuose. Ankstyvieji tyrimai pirmiausia orientavosi į kompiuterių operacinių sistemų saugumo patikrinimus, o įvairūs kibernetinio saugumo atakų tipai nebuvo aptarinėjami. Pirmasis kibernetinių išpuolių tyrimas atsirado devintojo dešimtmečio pradžioje, tuo pačiu metu, kai kibernetiniai nusikaltėliai pirmą kartą „iškilo į viešumą“ (Meyers ir kt., 2009).

Viena pagrindinių problemų, susijusi su kibernetinių grėsmių tyrimu, mokslininkų buvo siejama su pačios „kibernetinės atakos“ sąvoka, kuri yra labai plati ir gali apimti atakos vektorių, operacinių sistemų pažeidžiamumus, aparatinės ir programinės įrangos silpnybes, užpuolikų tikslus ir kt. Praktiškai neįmanoma sukurti sistemos, kuri numatytų savyje visus šios aspektus ir tuo pačiu metu išliktų logiška ir neperkrauta (Hansman, Hunt, 2003).

Per pastaruosius tris dešimtmečius mokslininkai atliko labai daug tyrimų ir pristatė didelį kiekį elektroninių grėsmių klasifikavimo sistemų. Kai kurie tyrimai yra grindžiami skirtingais įsilaužimo proceso etapais, o kiti – konkrečiais tikslais. Pavyzdžiui, C. Landwehr sukūrė kompiuterių saugumo pažeidžiamumų atsiradimo taksonomiją (Landwehr ir kt., 1994), J. Howard ir T. Longstaff pateikė kompiuterinių tinklų ir kibernetinių atakų taksonomiją (Howard, Longstaff, 1998), N. Weaver – kompiuterinių „kirminų“ taksonomiją (Weaver ir kt., 2003), S. Hansman ir R. Hunt – tinklų ir atakų taksonomiją (Hansman, Hunt, 2003), M. M. Kjaerland pristatė saugumo incidentų taksonomiją bei lygino incidentus viešajame ir privačiame sektoriuose (Kjaerland, 2006), N. Gruschka ir M. Jensen – išpuolių prieš debesų sistemas taksonomiją (Gruschka, Jensen, 2010). Kiti pasaulio mokslininkai taip pat pateikė savo klasifikavimo sistemas, kurios buvo skirtos konkrečioms technologijoms: DDoS (*angl. Distributed Denial of Service*), ugniasienių (*angl. Firewall*) atakoms ir kt.

Dauguma mokslininkų savo klasifikavimo sistemose daugiausia dėmesio skyrė hierarchinei taksonomijai, skirtai pirmiesiems kibernetinių įvykių padariniams: atakos vektoriams, pažeidžiamumams ir jų išnaudojimo galimybėms, įvertinti. Pirmieji mokslininkai, pasiūlę vertinti kibernetinių atakų poveikį objektui bei vieno tyrimo metu suklasifikavę kibernetinio incidento sukėlėjus ir jų motyvaciją, buvo J. Howard ir T. Longstaff, o jų sukurta taksonomija yra aktuali ir dabartiniu laikotarpiu (Ferdinand, Benham, 2017; Harry, 2018).

J. Howard ir T. Longstaff kompiuterinių incidentų taksonomiją sukūrė tyrimo, kuris buvo pradėtas kaip bandymas sukurti programinės įrangos pažeidžiamumų, dėl kurių gali kilti kompiuterinė ataka, klasifikavimo sistemą. 1998 metais mokslininkai pristatė pirmąjį bandymą sukurti bendrą saugumo taksonomiją. Ši taksonomija bandė apibrėžti kompiuterinį išpuolį, klasifikuodama jį pagal: išpuolio metu naudojamas technologijas (įrankius) (*angl. tools*); atakai išnaudojamus pažeidžiamumus; atakos vykdymo metodus; atakos tikslą ir atakos metu pasiektus rezultatus (Howard, Longstaff, 1998).

Taksonomija yra klasifikavimo sistema, kuri pertvarko žinių kryptį ir apibrėžia sistemos dalių tarpusavio santykį. Klasifikavimas – tai procesas, kurio metu taksonomijos principai panaudojami elementams atskirti ir grupuoti. J. Howard ir T. Longstaff, kurdami savo kompiuterinių incidentų taksonomiją, vadovavosi teorinėmis žiniomis, bet, siekdami taksonomijos visapusiškumo, logiškumo ir pritaikomumo, pasitelkė Reagavimo į kompiuterių incidentus koordinacinio centro (*angl. Computer Emergency Response Team Coordination centre (CERT/CC)*) praktinę patirtį. CERT/CC praktinės žinios ir naudojamas incidentų klasifikavimas buvo naudojamas taksonomijai patikslinti ir išplėsti (Howard, Longstaff, 1998). Ši simbiozė, pasak autorių, leido sukurti taksonomiją, kurioje naudojami terminai buvo suprantami bendrinę (kasdienę) kalbą naudojantiems visuomenės atstovams, o ne tik technologijų srities specialistams.

Kurdami savo taksonomija, J. Howard ir T. Longstaff manė, kad gera (patenkinama) taksonomija turi turėti klasifikavimo kategorijas (požymius), kurios atitinka tam tikras charakteristikas (Howard, Longstaff, 1998):

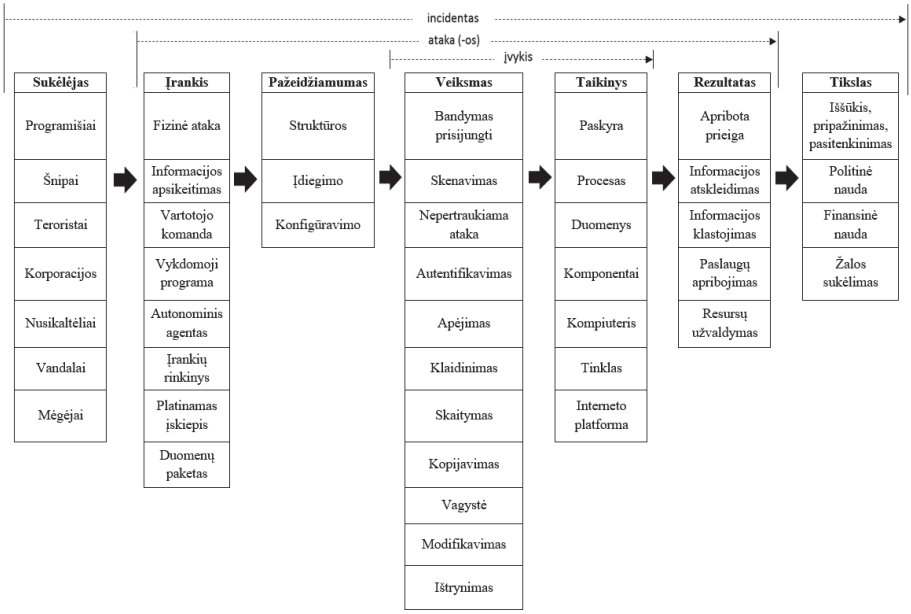
1. tarpusavio nesuderinamumas – vienai kategorijai priskiriami elementai negali būti priskiriami kitoms kategorijoms, nes kategorijos nesuderinamos;
2. išsamumas – sujungus visas kategorijas, kartu jos apims visumą;
3. nedviprasmiškumas – aiškus ir tikslus klasifikavimas, neatsižvelgiant į tai, kas yra klasifikuojama;
4. pakartojamumas – pakartotinas klasifikavimas lemia tą patį rezultatą, neatsižvelgiant į tai, kas yra klasifikuoja;
5. priimtinumas – logiškumas ir intuityvus supratimas, kad kategorijos galėtų tapti priimtinos daugumai;
6. naudingumas – gali būti naudojama, siekiant sužinoti apie tiriamąją sritį.

Kaip jau buvo minėta anksčiau, J. Howard ir T. Longstaff, kurdami savo klasifikavimo sistemą, bandė išanalizuoti kibernetinius incidentus ir atakas sąlygojančius faktorius bei pateikti visuomenei suprantamą kompiuterinių tinklų ir kibernetinių incidentų taksonomiją.

J. Howard ir T. Longstaff taksonomijoje naudojamos trys pagrindinės sąvokos: įvykis, ataka ir incidentas (Howard, Longstaff, 1998):

- *įvykis* apibrėžiamas kaip veiksmas, nukreiptas į tam tikrą taikinį, siekiant pakeisti taikinio, į kurį nukreiptas veiksmas, būseną;
- *ataka* – veiksmų seka, kuria objektą atakuojantys asmenys pasiekia tam tikrą tikslą (neteisėtą rezultatą);
- *incidentas* – atakų grupė, kurią galima išskirti iš kitų atakų visumos, pasinaudojant būtent tai grupei būdingais požymiais: atakuojamųjų objektų savybės, atakų vykdymo metodas, siekiami tikslai, vieta ir laikas.

J. Howard ir T. Longstaff kompiuterinių incidentų taksonomija pavaizduota 4 paveiksle.



Šaltinis: *Howard, Longstaff, 1998*

4 paveikslas. *J. Howard ir T. Longstaff kompiuterinių incidentų taksonomija*

Bet koks kibernetinis saugumo incidentas gali būti suprantamas kaip procesas, kuris turi tam tikrą iniciatorių (kibernetinį nusikaltėlį ar jų grupę), kuris naudojasi tam tikrais įrankiais ir žiniomis, siekdamas neteisėtai paveikti informacinius išteklius (ataka), su tikslu gauti tam tikrą naudą. Incidento metu jo iniciatorius gali naudoti ne vieną ataką, o derinti jas tarpusavyje, kol pasieks užsibrėžtą tikslą arba kol incidentas bus pastebėtas ir informacinių išteklių savininkas sugebės sėkmingai atremti kibernetines atakas.

Pristatant kibernetinio saugumo taksonomiją elektroninių rinkimų sistemų kontekste, šiame disertaciniame darbe bus naudojama J. Howard ir T. Longstaff kompiuterinių incidentų taksonomija, kuri bus koreguojama ir tobulinama, atsižvelgiant į šiuolaikines technologijas, kibernetinių incidentų raidą bei pažeidžiamumus, kurie kyla elektroninėms balsavimo sistemoms.

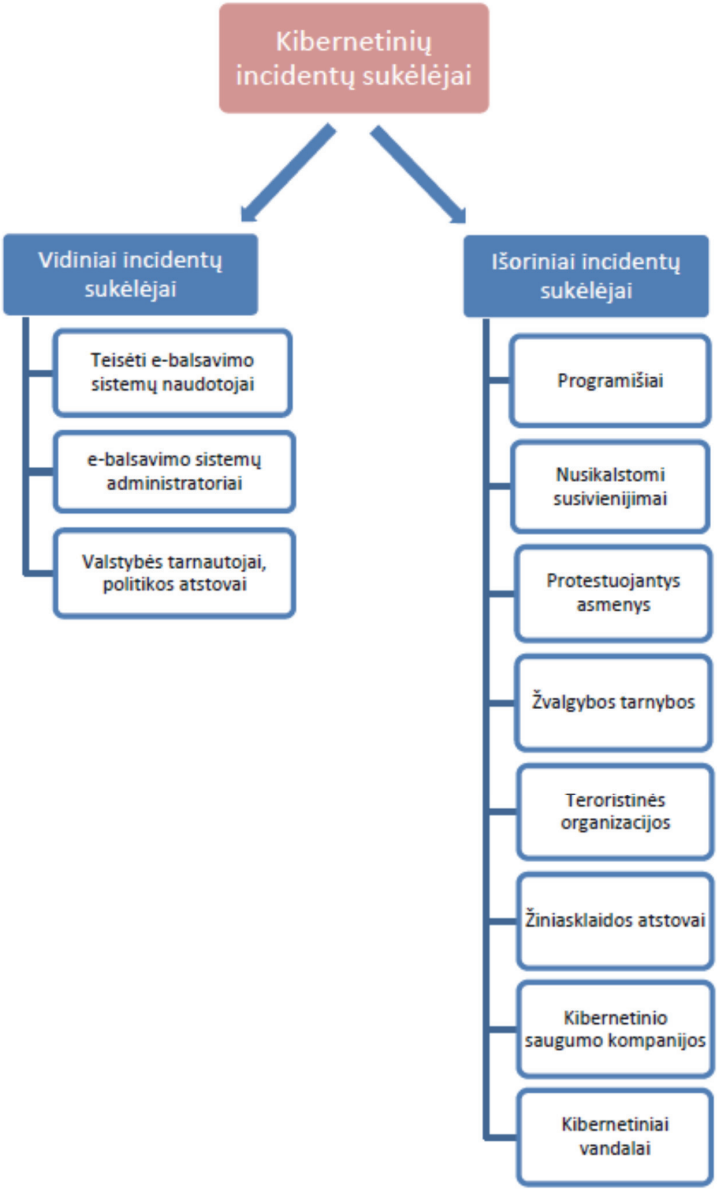
1.4.1. Kibernetinių incidentų sukėlėjai

J. Howard ir T. Longstaff savo kibernetinių incidentų ir kompiuterinių tinklų taksonomijoje pateikė septynias kibernetinių incidentų sukėlėjų kategorijas: programišiai (*angl. hacker*); žvalgybos tarnybų darbuotojai (šnipai); teroristinių organizacijų atstovai; darbuotojai, pasamdyti vykdyti kompiuterines atakas prieš konkurentus (korporacijos); nusikalstomos grupuotės (nusikalteliai); vandalai; asmenys, siekiantys įgauti moralinį pasitenkinimą (mėgėjai) (Howard, Longstaff, 1998).

Šiame disertaciniame darbe kibernetinių incidentų sukėlėjai bus skirstomi į dvi stambias grupes – vidiniai ir išoriniai kibernetinių incidentų sukėlėjai. Incidentų sukėlėjų suskirstymas detaliau pavaizduotas 5 paveiksle.

Vidinių kibernetinių incidentų sukėlėjų grupė skirstoma į:

1. *teisėtus elektroninių balsavimo sistemų naudotojus* (pvz., valstybės piliečiai), kurie gali ieškoti pažeidžiamumų ir / arba saugumo spragų elektroninių rinkimų sistemose bei, turėdami pakankamai techninių žinių ir tinkamą motyvaciją, gali sukelti kibernetinius incidentus elektroninio balsavimo sistemose;
2. *elektroninių balsavimo sistemų valdytojai* (pvz., sistemų administratoriai, kompiuterinius tinklus aptarnaujantys darbuotojai), kurie gali siekti pasinaudoti elektroninių balsavimo sistemų valdytojų privilegijuotomis pozicijomis tam, kad pasinaudotų pažeidžiamumais elektroninio balsavimo sistemose. Prie šios grupės taip pat gali būti priskiriami valstybės tarnautojai arba kitų organizacijų darbuotojai, kurie dalyvauja elektroninio balsavimo sistemų kūrimo, diegimo ar priežiūros procesuose. Tokie asmenys gali turėti pakankamai informacijos ir žinių, kad atliktų neteisėtus veiksmus ir įsilaužtų į elektronines balsavimo sistemas;
3. *valstybės tarnautojai ar politinių partijų atstovai*, kurie, pasinaudodami savo politinėmis galiomis ar asmeninėmis pažintimis, gali daryti įtaką elektroninių balsavimų sistemoms, nors ir nėra tiesiogiai susiję su elektroninių balsavimų sistemų diegimu ar aptarnavimu. Šie asmenys gali daryti įtaką ir veikti per kitus asmenis, tokiu būdu dalyvaudami įsilaužimuose ar vadovaudami elektroninių balsavimo sistemų atakoms (Limba, Agafonov, 2012).



Šaltinis: *sudaryta autoriaus*

5 paveikslas. *Kibernetinių incidentų sukėlėjai*

Pasak V. Augoye ir A. Tomlinson (cit. Schneier, 2009), vidinių kibernetinių incidentų sukėlėjų vykdoma veikla yra ypač žalinga, kadangi šiais asmenimis yra pasitikima ir jie dažniausiai turi prieigą prie informacinių išteklių (Augoye, Tomlinson, 2018). Turėdami galimybę pasiekti informacinius išteklius, taip pat žinodami, kaip visa informacinė sistema veikia (kadangi jie dalyvavo kuriant ar diegiant sistemą), vidiniai kibernetinių incidentų sukėlėjai pridaro ypač daug žalos, nes jie jau yra sistemos viduje, o tai apsunkina jų aptikimą ir galimybę apsisaugoti nuo jų vykdomos ardomosios veiklos. V. Augoye ir A. Tomlinson taip pat pažymi, kad kibernetiniai incidentai, kurie vyksta dalyvaujant vidiniams grėsmių sukėlėjams, yra viena iš didžiausių grėsmių, kylančių organizacijos informaciniams ištekliams (Augoye, Tomlinson, 2018).

Išorinių kibernetinių incidentų sukėlėjų grupė skirstoma į:

1. *programišiai* (*angl. hackers*) – asmenys, ieškantys elektroninių balsavimo sistemų saugumo spragų ar galimybės neigiamai paveikti elektronines balsavimo sistemas. Šie asmenys dažniausiai ieško galimybės gauti prieigą prie elektroninių balsavimo sistemų ar jose saugomų duomenų. Dabartiniu laikotarpiu žodis *programišius* dažniausiai turi neigiamą prasmę ir naudojamas, siekiant bendrai apibrėžti visus asmenis, siekiančius sukelti kibernetinius incidentus ir iš šios veiklos gauti naudą. Tačiau J. Howard ir T. Longstaff savo taksonomijoje šiam terminui nesuteikė neigiamos prasmės. Šiame darbe terminas *programišius* suprantamas taip, kaip jį apibrėžia *Enciklopedinis kompiuterijos žodynas*: „asmuo, kuriam labai patinka programuoti, nagrinėti operacinių sistemų ir kitų programų pirminius tekstus, juos tobulinti“ (Dagienė ir kt., 2014);
2. *nusikalstamos organizacijos ir / arba pavieniai nusikaltėliai*, kurie vykdo įsilaužimus į elektroninio balsavimo sistemas arba siekia pasisavinti šiose sistemose kaupiamą informaciją;
3. *protestuojančių asmenų grupės* arba *hacktivistai*, kurie gali bandyti vykdyti elektroninių balsavimo sistemų atakas tam, kad pademonstruotų priešiškumą šių sistemų panaudojimui balsavimo procesuose arba įrodytų naudojamų technologijų ir balsavimo procesų nesaugumą, bet neturi tikslo padaryti sistemoms fizinės žalos. Šios asmenų grupės dažniausiai išreiškia savo poziciją per žiniasklaidos priemones, socialinius tinklus (Donaldson ir kt., 2015; Rozumski, 2016);
4. *užsienio žvalgybų tarnybos,* kurios gali būti suinteresuotos gauti informacijos apie balsuojančius asmenis ir balsavimo rezultatus. Dažnai šių tarnybų vykdoma veikla yra nukreipta į elektroninių rinkimo sistemų rezultatų klastojimą arba į elektroninio balsavimo sistemose balsavimo metu kaupiamą informaciją. Šie veiksmai gali būti panaudojami, siekiant suprasti, kokios yra balsavimo intencijos ir, esant reikalui, daryti įtaką balsavimo rezultatams arba trikdyti balsavimo procesą. Taip pat gauta informacija gali būti naudinga, siekiant patobulinti tam tikrų kandidatų rinkiminę kampaniją bei manipuliuoti visuomenės nuomone (Limba, Agafonov, 2012; Donaldson ir kt., 2015; Johnson, 2015; CCDCOE, 2016; Williams, 2016);
5. *teroristinės organizacijos* gali būti suinteresuotos surinkti informacijos apie privačius asmenis, kuri yra saugoma elektroninio balsavimo sistemose. Šios

organizacijos, naudodamos turimas žinias, galėtų šnipinėti arba rengti teroro aktus, kitaip bauginti visuomenę (Limba, Agafonov, 2012);

6. žiniasklaidos atstovai, kurie gali domėtis elektroninių balsavimo sistemų spragomis, siekdami parengti reportažą (atlikti žurnalistinį tyrimą) bei padidinti visuomenės susidomėjimą elektroninėmis balsavimo sistemomis. Dažnai tokie žurnalistiniai tyrimai nėra skirti teigiamoms elektroninio balsavimo sistemų galimybėms viešinti, o sistemų analizė vykdoma tam, kad būtų įrodytas elektroninio balsavimo netobulumas;
7. *kibernetinio saugumo programinės ir techninės įrangos gamintojai* (kompanijos) taip pat gali būti suinteresuoti elektroninių balsavimo sistemų pažeidžiamumais. Dažnas motyvas yra konkurencinė kova su kitais to paties sektoriaus produkciją gaminančiais verslininkais. Šios grupės, vykdydamos išpuolius prieš elektronines balsavimo sistemas, gali atlikti sistemų pažeidžiamumų testus (*angl. penetration tests*), tačiau visa esmė slypi tame, kokiam tikslui ir kaip gauti duomenys bus panaudojami toliau;
8. *kibernetiniai vandalai,* kurie įsilaužia į elektronines balsavimo sistemas ir trikdo sistemų darbą arba gadina jose kaupiamą informaciją.

1.4.2. Kibernetinių incidentų sukėlėjų tikslai

J. Howard ir T. Longstaff, pristatydami pasauliui savo kibernetinių incidentų ir kompiuterinių tinklų taksonomiją, pažymėjo, kad žmonės, atakuodami kompiuterines sistemas, tai daro skirtingais metodais ir turi skirtingų tikslų (Howard, Longstaff, 1998):

- nori išbandyti savo jėgas ir galimybes (saviraiška), įgauti tam tikrą statusą tarp bendraminčių arba tiesiog jaučia vidinį pasitenkinimą dėl to, kad sugebėjo įvykdyti sėkmingą ataką prieš informacinius išteklius;
- siekia įgyti politinės galios ar pranašumų prieš kitus politinius oponentus;
- planuoja gauti finansinės naudos iš savo vykdomos veiklos;
- siekia pažeisti informacinėse sistemose saugomą informaciją ar sutrikdyti informacinių išteklių kasdienę standartinę veiklą.

Nagrinėjant kibernetinių incidentų sukėlėjų motyvaciją elektroninių rinkimų sistemų kontekste bei atsižvelgiant į šiuolaikinėje globalioje visuomenėje vykstančius pokyčius, galima sakyti, kad J. Howard ir T. Longstaff siūlomos tikslų kategorijos vis dar yra aktualios, bet jos gali būti papildytos socialinių problemų viešinimo (visuomenės pasipriešinimo, socialinio pasipriešinimo) kategorija. Šios elektroninių rinkimų kibernetinių incidentų taksonomijos incidentų sukėlėjų tikslai detaliau yra pavaizduoti 6 paveiksle, o jų aprašymas yra pateikiamas toliau.

Šaltinis: *sudaryta autoriaus*

6 paveikslas. *Kibernetinių incidentų sukėlėjų tikslai*

Kibernetinio saugumo incidentų elektroninėse balsavimo sistemose taksonomijoje incidentų iniciatorių tikslai, kaip ir buvo minėta anksčiau, yra skirstomi į penkias kategorijas:

1. *saviraiškos, pasitenkinimo, pripažinimo ir reputacijos siekimas*. Šio tikslo dažniausiai siekia: programišiai (Štitilis, 2011), teisėti elektroninio balsavimo sistemų vartotojai, žiniasklaidos atstovai (Limba, Agafonov, 2012) ir kibernetinio saugumo kompanijos. Šio tikslo siekiantys kibernetiniai įsilaužėliai dažnai sukelia kibernetinius incidentus ir vykdo kibernetines atakas be tikslo sugadinti

balsavimo sistemas. Aptikę tam tikras saugumo spragas ar pažeidžiamumus, dažniausiai apie tai praneša elektronines balsavimo sistemas administruojančioms organizacijoms, kurios turi galimybę užtikrinti aptiktų pažeidžiamumų šalinimą;

2. *politinės įtakos siekimas* yra būdingas: valstybės tarnautojams ir politinių partijų atstovams (Limba, Agafonov, 2012), žvalgybos tarnyboms ir teroristinėms organizacijoms. Visi šie kibernetinių incidentų sukėlėjai siekia politinės įtakos, bet šios įtakos siekimo išraiška yra skirtinga: pvz., tiesioginės politinės valdžios ir politinės įtakos siekimas būdingas politinių partijų atstovams ir valstybės tarnautojams, „tinkamesnio" valstybės politiko išrinkimas į svarbius politinius postus(mokslinėje literatūroje šis reiškinys charakterizuojamas kaip *kibernetinis lobizmas* (*angl. cyber lobby*)) (Stankevičius, Simanavičienė, 2016) būdingas žvalgybos tarnyboms ir teroristinėms organizacijoms (Limba, Agafonov, 2012);
3. *finansinės naudos gavimas*. Šio tikslo siekimas mokslinėje literatūroje yra siejamas su nusikalstamomis grupuotėmis ar pavieniais kompiuteriniais nusikaltėliais (Štitilis, 2011) bei su asmenimis, kurie tiesiogiai prižiūri elektronines balsavimo sistemas priežiūra, jas diegia ir kt. (Limba, Agafonov, 2012);
4. *elektroninių balsavimo sistemų ir sistemose saugomos informacijos sunaikinimas arba šių sistemų įprastos veiklos trikdymas*. Dažniausiai mokslinėje literatūroje ši veikla laikoma būdinga kibernetiniams vandalams (Howard, Longstaff, 1998; Štitilis, 2011);
5. *socialinių problemų ir / ar visuomenės nuomonės viešinimo* tikslas – tam tikrų pavienių asmenų ar asmenų grupių veiksmai, siekiant diskredituoti elektroninių rinkimų sistemas (Limba, Agafonov, 2012). Protestuojančių asmenų grupės gali bandyti atakuoti elektronines balsavimo sistemas tam, kad pademonstruotų savo priešiškumą šių sistemų panaudojimui rinkimų procese. Įvykdžius sėkmingus išpuolius prieš elektronines balsavimo sistemas, pranešimai apie aptiktus saugumo pažeidžiamumus yra tikslingai ištransliuojami į viešumą, pasinaudojant žiniasklaidos priemonėmis (pvz., naujienų portalais, socialiniais tinklais ir kt.). Tokiu būdu informacija apie pažeidžiamumus tampa žinoma plačiajai visuomenei ir prastėjanti elektroninių balsavimo sistemų „reputacija" formuoja neigiamą valstybės piliečių nuomonę apie šias sistemas, o patys elektroniniai rinkimai tampa nepatrauklūs, kadangi atrodo nepatikimi ir nesaugūs.

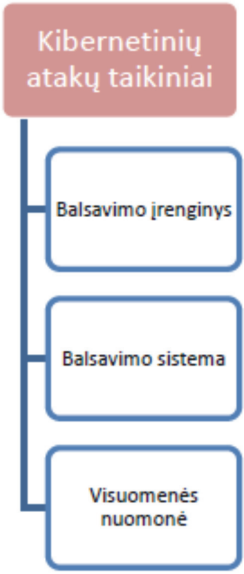
Pažymėtina, kad visi anksčiau įvardyti kibernetinių incidentų tikslai yra daugiau ar mažiau būdingi tam tikriems kibernetinių incidentų sukėlėjams, tačiau negalima kategoriškai teigti, kad užpuolikas, vykdydamas savo neteisėtą veiklą, siekia tam tikro konkretaus anksčiau įvardyto tikslo (Geers, 2015). Ryšys tarp elektroninės balsavimo sistemos užpuoliko klasifikavimo ir jo siekiamo tikslo yra dinamiškas ir gali pasikeisti kibernetinio incidento vykdymo metu, atsižvelgiant į incidento sukėlėjo tyčinius ar netyčinius veiksmus. Pavyzdžiui, programišius, siekdamas visuotinio pripažinimo, vykdo elektroninės rinkimų sistemos pažeidžiamumų paiešką ir, aptikęs saugumo spragas, nusprendžia, kad geriausiai apie šias spragas bus pranešti viešai, pasinaudojant socialiniais tinklais. Tokiu būdu paviešindamas pranešimą, jis gali tiesiogiai veikti

valstybės piliečių nuomonę apie elektroninių balsavimų sistemų saugumą ir pasitikėjimą sistema, o savo netyčiniais veiksmais kibernetinio incidento metu transformuoti kibernetinio saugumo incidento tikslą.

1.4.3. Elektroninių rinkimų sistemų kibernetinės atakos

Elektroninių rinkimų sistemų kibernetinės atakos gali būti skirstomos į tris stambias grupes, kurios yra nustatomos pagal atakos taikinio charakteristiką (žr. 7 paveikslą):

1. *Poveikis elektroninio balsavimo įrenginiams* (technologinės asmeninių rinkėjų ar rinkimų apylinkėse naudojamų balsavimo įrenginių atakos);
2. *Poveikis elektroninio balsavimo sistemoms* (technologinės atakos, kurių tikslas yra pakenkti balsavimo sistemoms, sistemose saugomiems bei į jas perduodamiems duomenims arba trikdyti balsavimo sistemų stabilų veikimą);
3. *Elektroninių balsavimo sistemų patrauklumo mažinimas*. Ne technologinės, informacijos sklaidos kibernetinės atakos, kurių tikslas yra kompromituoti elektronines balsavimo sistemas, sukeliant visuomenės nepasitikėjimą elektroninio balsavimo procesu arba rezultatais.



Šaltinis: *sudaryta autoriaus*

7 paveikslas. *Kibernetinių atakų taikiniai*

Poveikis elektroninio balsavimo įrenginiams. Elektroninius vartotojo balsavimo sistemos įrenginius, naudojamus elektroninio balsavimo procese, galima suskirstyti į dvi grupes: asmeniniai naudotojų balsavimo įrenginiai (asmeniniai kompiuteriai, telefonai) ir valstybės naudojami bei kontroliuojami (prižiūrimi) balsavimo įrenginiai (elektroninės

balsadėžės), kuriomis elektroninis balsavimas vykdomas rinkiminėse apylinkėse. Labiausiai tikėtinos kibernetinės atakos prieš balsavimui panaudojamus įrenginius (asmeninius ir valdomus atsakingų už balsavimus institucijų) bus įvardijami toliau.

Mokslininkai savo tyrimuose dažnai pabrėžia, kad pati didžiausia kibernetinė elektroninių balsavimo sistemų grėsmė yra susijusi su balsavimui naudojamų vartotojų asmeninių įrenginių pažeidžiamumais, kadangi būtent asmeniniai vartotojų įrenginiai yra labiausiai pažeidžiami dėl menkos priežiūros (Jefferson ir kt., 2004; Alvarez, 2010; Springall ir kt., 2014). Tokiems pažeidžiamumams išnaudoti kibernetiniai nusikaltėliai pasitelkia *kenkėjišką programinę* įrangą (*angl. malware*), kuri naudojama, organizuojant technologines elektroninių balsavimo sistemų atakas.

Kenkėjiška programinė įranga yra viena iš dažniausiai pasitaikančių kibernetinių incidentų priežasčių. Dažnai kenkėjiška programinė įranga yra tapatinama su kompiuteriniais virusais, bet realybėje kenkėjiškos programinės įrangos sąvoka yra daug platesnė (Johnson, 2015; Subrahmanian ir kt., 2015; Cucu, 2017). Pasak P. Cucu, *ne kiekviena kenkėjiška programinė įranga yra kompiuterinis virusas, bet kiekvienas kompiuterinis virusas yra kenkėjiška programa* (Cucu, 2017).

Prie kenkėjiškos programinės įrangos yra priskiriami:

- *Kompiuteriniai virusai* – programinė įranga, kuri pažeidžia elektroniniams rinkimams naudojamus įrenginius arba elektroninių balsavimo sistemų serverius ir apsunkina balsavimo procesą arba visiškai sutrikdo balsavimo sistemų darbą. Kompiuteriniai virusai veikia kaip ir gamtoje egzistuojantys virusai ir siekia daugintis per visus įmanomus komunikacijos kanalus bei užkrėsti kuo daugiau aplinkoje esančių kompiuterių. Prie kompiuterinių virusų taip pat gali būtų priskiriamos ir „loginės arba laiko bombos“, kurios aktyvuojasi ir vykdo savo programiniame kode numatytas funkcijas tam tikru laiku;
- *Trojos arkliai* – savaime nesidauginanti kenkėjiška programinė įranga, kurios veikimas yra maskuojamas, pasinaudojant kitomis programomis, kurių veikimas gali būti naudingas, bet tuo pačiu yra įdiegiami neaprašyti programinės įrangos paketai ar papildomos programos funkcijos, kurios, pavyzdžiui, gali stebėti ir įrašinėti vartotojo veiksmus. Taip pat *Trojos arklių* programinės įrangos grupei gali būti priskiriama programinė įranga, skirta nutolusiam kompiuteriui valdyti. Jei kibernetiniam nusikaltėliui pavyksta įdiegti tokio tipo programinę įrangą, tai vartotojo kompiuteris tampa ne tik kibernetinio nusikaltimo taikiniu, bet ir, nežinant vartotojui, gali būti naudojamas kaip nusikaltimo vykdymo įrankis (dalis *botnet* tinklo), organizuojant atakas prieš kitus informacinius išteklius;
- Šnipinėjimo programos (*angl. spyware*) – programinė įranga, stebinti visus vartotojo veiksmus, juos įrašanti ir perduodanti duomenis programinės įrangos „savininkui“;
- *Rootkit* programinės įrangos paketai, kurių pagrindinis tikslas yra infekuoti kompiuterines sistemas aparatūriniame lygmenyje. Šios programos užkraunamos į kompiuterines sistemas dar prieš visą operacinės sistemos pakrovimą ir dažnai yra neaptinkamos antivirusinėms programoms, o veikdamos gali įtraukti kompiuterius į *botnet* tinklus, naudojamus kibernetinėms atakoms, arba maskuoti kitos kenkėjiškos programinės įrangos veikimą;

- *Parsisiuntimo atakų programinė įranga* (*angl. drive-by download*), kurios pagrindinis tikslas yra parsisiųsti programinės įrangos paketus į vartotojo kompiuterį, į parsisiuntimo procesą neįtraukiant vartotojo. Tokia programinė įranga dažniausiai yra įskiepijama į kompromituotas interneto svetaines, o kompiuterio naudotojas dažnai net nežino, kad kažką parsisiuntė. Vėliau į kompiuterį yra parsiunčiama piktavalių paruošta pažeidžiamumų skenavimo programinė įranga, kuri atlieka skenavimą ir, aptikusi pažeidžiamumą kompiuterinėje sistemoje, pasinaudoja juo, infekuodama aukos kompiuterinę sistemą;
- *Ransomware* programinė įranga, kurios pagrindinis tikslas – užšifruoti kompiuteriuose ar kompiuterinėse sistemose esančius duomenis ir iš sistemos savininko reikalauti mokesčio už duomenų iššifravimą.

Pažymėtina, kad kenkėjiškos programinės įrangos poveikis balsavimo įrenginiams negali būti tapatinamas išskirtinai tik su asmeninių kompiuterių (vartotojo elektroninių įrenginių) pažeidžiamumais. Elektroninės balsadėžės taip pat gali būti paveikiamos, panaudojant kenkėjišką programinę įrangą, įdiegiant ją į elektroninius balsavimo įrenginius (Siliconrepublic.com, 2006; Kiayias ir kt., 2006), bet tokiam efektui pasiekti dažniausia yra reikalinga fizinė prieiga prie balsavimo įrenginių.

Prie vartotojo įrenginių kibernetinių atakų taip pat gali būti priskiriamos:

- *elektromagnetinio spinduliavimo spektro atakos* (*angl. TEMPEST*). Šių atakų pagrindinis tikslas – per atstumą nuskaityti informaciją, kuri nuskaitymo metu apdorojama įrenginyje. Tokio tipo atakos gali būti naudojamos, siekiant kompromituoti elektroninį balsavimą visuomenėje, nes nėra galimybės išsaugoti balsavimo proceso slaptumo. Apibūdinant elektromagnetinio spinduliavimo spektro atakų naudojimą, galima teigti, kad šios atakos gali būti naudojamos prieš elektroninio balsavimo įrenginius, esančius rinkiminėse apylinkėse, arba prieš elektroninių balsavimų sistemų kamieninę įrangą, kadangi organizuoti tokio tipo atakas prieš pavienius kompiuterius yra neefektyvu informacijos kiekio išgavimo ir kaštų kontekste;
- *DNS atakos* (*angl. Domain Name System*). Pasauliniame interneto tinkle interneto svetainėms identifikuoti yra naudojamos skaitmenų grupės, kurios yra vadinamos IP (*angl. Internet Protocol*) adresais. Siekiant patogumo ir paprastesnio interneto svetainių adresų naudojimo, IP adresai yra transformuojami į žodžius ar ženklus, kuriuos vartotojas įveda į interneto naršymo programos adreso lauką ir tokiu būdu pasiekia norimą svetainę. Svetainės pavadinimo transformacija į IP adresą yra vykdoma *domeno vardų serveriuose* (*angl. Domain Name Server (DNS)*), kuriuose ir saugoma informacija apie svetainės pavadinimo atitikmenį IP adresui. Vykdant DNS atakas, kibernetinių incidentų sukėlėjai klastoja DNS įrašus ir nukreipia vartotojus į netikras svetaines. Internetinio balsavimo metu incidentų sukėlėjai gali sukurti netikras balsavimui skirtas svetaines ir, pasinaudodami DNS atakomis, nukreipti į jas balsuojančius asmenis. Tokiu būdu nusikaltėliai gali siekti surinkti informaciją apie balsuojančius asmenis (prisijungimo duomenys, slaptažodžiai ir kt.), trukdyti piliečiams pareikšti savo nuomonę rinkimuose arba klastoti jų balsus. Pažymėtina, kad DNS atakos yra skirtos vartotojų srautui

į netikras svetaines nukreipti, bet vartotojo asmeninis įrenginys nėra tiesiogiai pažeidžiamas šios atakos metu;

- *Interneto svetainių klastojimo ataka* (*angl. Website spoofing attack*). Šios atakos metu piktavaliai sukuria elektroninių balsavimų metu naudojamą interneto svetainę, kuri gali visiškai identiškai atkartoti oficialią balsavimo internetu svetainę. Vartotojas, patekęs į šiuos spąstus, vykdo balsavimo procedūrą jam įprastu metodu, net neįtardamas, kad jo pareikšta valia nėra fiksuojama oficialių rinkimų metu. Pagrindinis šios atakos tikslas yra visais įmanomais būdais neleisti rinkėjui balsuoti oficialiuose rinkimuose, taip pat pažeisti rinkimų slaptumą.

Apibendrinant galima teigti, kad kibernetinių incidentų sukėlėjai, siekdami paveikti elektroninius rinkimus, gali bandyti pasinaudoti kenkėjiška programine įranga ir paveikti potencialių rinkėjų balsavimui naudojamus įrenginius. Tačiau šios programinės įrangos panaudojimo grėsmė taip pat yra taikoma ir techninei bei programinei įrangai, kuri yra skirta elektroninių balsavimo sistemų veiklai užtikrinti. Į šias sistemas taip pat gali patekti kenkėjiška programinė įranga, nors šios sistemos gali neturėti ryšio su pasauliniu interneto tinklu. Dažniausiai kibernetiniai nusikaltėliai siekia visais įmanomais būdais priversti auką vykdyti nusikaltėliams palankius veiksmus, o išpuoliai prieš vartotoją (vartotojo naudojamus įrenginius) ar sistemas sujungia kelis kibernetinių atakų vektorius: socialinę inžineriją, kenkėjišką programinę įranga ir kt. (CCDCOE, 2016).

Poveikis elektroninio balsavimo sistemoms. Šiame disertaciniame darbe poveikis elektroninio balsavimo sistemoms suprantamas kaip technologinės kibernetinės atakos, kurių tikslas sutrikdyti balsavimo sistemų darbą, atliekant tiesioginį įsibrovimą į balsavimo sistemas, apsunkinant vartotojų prieigą prie sistemos ar sistemoje naudojamų įrenginių. Kibernetinėms atakoms prieš elektronines balsavimo sistemas dažniausiai yra priskiriamos šios atakos:

- *Ataka balsavimo biuletenio siuntimo metu* (ataka dar kartais vadinama žmogus viduje (*angl. man-in-the-middle*)), kurios tikslas yra perimti rinkėjo įrenginio siunčiamą balsavimo biuletenį ir, atsižvelgiant į kibernetinio incidento sukėlėjo tikslą, modifikuoti, sugadinti ar atskleisti siunčiamą balsą. Vykdant šią ataką internetinio balsavimo kontekste, gali būti siekiama tik „nepalankių balsų“ ribojimo, tokiu būdu siekiant padidinti „tinkamo kandidato“ pranašumą prieš politinius oponentus. Pažymėtina, kad, vykdant balsavimo biuletenių siuntimo ataką elektroninių rinkimų kontekste (t. y. atakuojant elektroninių balsadėžių siunčiamus duomenis), gali būti naudojamos dvi skirtingos taktikos, kurios priklauso nuo procesų, naudojamų rinkimų sistemose (balsavimo sistemos konfigūracijos):
  1. jei elektroninės balsadėžės persiunčia kiekvieną rinkėjo atiduotą balsą į balsų skaičiavimo sistemą realiu laiku, gali būti siekiama modifikuoti, sugadinti ar atskleisti siunčiamą balsą;
  2. jei elektroninė balsadėžė kaupia visus balsus ir po rezultatų skaičiavimo į balsų skaičiavimo sistemą siunčia tik apibendrintus rezultatus, gali būti siekiama modifikuoti bendrą rezultatą, pakeičiant jį taip, kad jis būtų naudingas tam tikram kandidatui;

- Teikiamų sistemos *paslaugų ribojimo ataka* (*angl. Denial of Service*) ir *paskirstyta paslaugų ribojimo ataka* (*angl. Distributed Denial of Service*). Šių atakų pagrindinis tikslas yra sukurti tokias sąlygas, kad teisėtiems elektroninio balsavimo sistemos naudotojams sistemų teikiamos paslaugos būtų neprieinamos arba naudojimasis šiomis paslaugomis būtų apsunkintas ir nepatogus vartotojui. Kibernetinio incidento sukėlėjui vykdant šio tipo atakas ir apkraunant elektroninę balsavimo sistemą, galima sutrikdyti normalų balsavimo sistemos veikimą ir kompromituoti elektronines balsavimo sistemas (rinkimus). Vykdydami tokio tipo atakas, piktavaliai dažniausiai naudojasi iš anksto paruoštais *kompiuteriais zombiais*, kurie yra valdomi ir sujungti į tinklus (*angl. botnet*) (Johnson, 2015). Tokius kompiuterių tinklus galima nusipirkti arba išsinuomoti juodojoje rinkoje, o šių tinklų panaudojimas tampa viena iš dažniausiai sutinkamų kibernetinių grėsmių (Kacha, 2014). Tačiau reikia atkreipti dėmesį, kad išlieka grėsmė, kad šio tipo kibernetinės atakos gali atsirasti ir kibernetinių incidentų sukėlėjams nedalyvaujant. Neteisingai apskaičiuoti sistemos technologiniai parametrai, neapgalvotas ryšio kanalų pralaidumo pasirinkimas ir netinkamai įvertintas teisėtų vartotojų naudojimosi sistema mastas taip pat gali sukelti paslaugų ribojimą informaciniuose ištekliuose;
- *Interneto svetainių gadinimas* (*angl. WEB page defacing*). Kibernetinis išpuolis prieš elektroninių rinkimų sistemas, siekiant sugadinti interneto svetaines, kurios reprezentuoja elektroninius rinkimus arba kurios vykdo internetinį balsavimą. Šios atakos dažnai nesukelia didelių finansinių nuostolių, bet turi psichologinį poveikį visuomenei, kadangi dauguma piliečių nesusimąsto apie tai, kad, pvz., Vyriausiosios rinkimų komisijos interneto svetainės talpinimo paslaugas tiekia komercinė organizacija, o įsilaužimas į komercinės organizacijos serverius dažniausiai parodo kibernetinio saugumo problemą šioje organizacijoje, o ne Vyriausioje rinkimų komisijoje. Tokiu būdu gali būti formuojama neigiama nuomonė apie internetinius rinkimus, taip pat apie elektronines balsavimo sistemas;
- *Nulinės dienos atakos* (*angl. Zero-Day attacks*). Šios atakos yra priskiriamos prie pačių pavojingiausių pažeidžiamumų išnaudojimų, o jų realizavimo mechanizmas yra grindžiamas programinės įrangos (operacinių sistemų ir taikomosios programinės įrangos) saugumo spragomis. Atrastas saugumo spragas išnaudoja kibernetinių incidentų sukėlėjai, o programinės įrangos gamintojas dažnai net nežino apie šių spragų egzistavimą. Nulinės dienos atakos gali būti skirstomos į tris grupes:
  1. nulinės dienos atakos, išnaudojančios pažeidžiamumus, kai informacija apie pažeidžiamumą tampa viešai žinoma ir yra išleisti programinės įrangos atnaujinimai (pataisymai), kurių įdiegimas panaikina pažeidžiamumą (nulinė diena);
  2. nulinės dienos atakos, išnaudojančios saugumo pažeidžiamumus, kurie nebuvo „pataisyti“, bet informacija apie pažeidžiamumus yra paviešinta;
  3. nulinės dienos atakos, išnaudojančios saugumo pažeidžiamumus, kurie nebuvo „pataisyti“, bet informaciją apie pažeidžiamumus nėra paviešinta. Tokios atakos dar kartais vadinamos mažesnės nei nulinės dienos atakos (*angl. less than zero-day attacks*).

Nulinės dienos pažeidžiamumų paieškas programinėje įrangoje gali atlikti įvairūs veikėjai: kibernetinio saugumo ekspertai ar kompanijos, mokslininkai, kibernetiniai nusikaltėliai, informacinių sistemų naudotojai arba programinės įrangos gamintojai. Jei pažeidžiamumai yra aptinkami „gerų vyrukų“ pastangomis, tai dažnai jie yra nežinomi iki tol, kol programinės įrangos spragos nėra pataisomos arba vartotojai nėra įspėjami apie jų tykančias grėsmes. Tačiau kartais informacinių sistemų naudotojų aptikti saugumo pažeidžiamumai yra paviešinami visuomenės informavimo priemonėse. Tokiu būdu sąmoningai ar nesąmoningai pažeidžiamumą aptikęs asmuo pradeda „kibernetines rungtynes“ tarp kibernetinių nusikaltėlių ir programinės įrangos gamintojų (kibernetinio saugumo ekspertų): ar pažeidžiamumas bus panaikintas (pataisytas) greičiau nei nusikaltėliai sugalvos pažeidžiamumo išnaudojimo būdą.

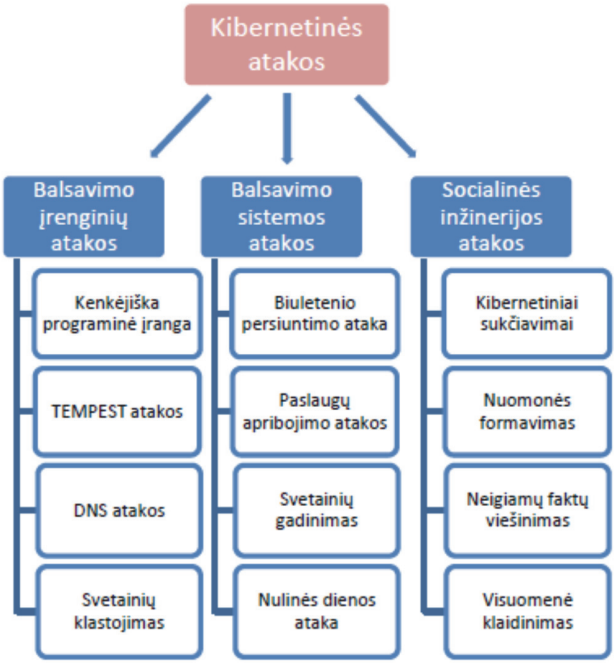
Elektroninių balsavimo sistemų patrauklumo mažinimas. Elektroninių balsavimo sistemų patrauklumo mažinimo atakas galima susieti su *socialinės inžinerijos atakomis,* kurias naudoja kibernetinių incidentų sukėlėjai ir kurios yra grindžiamos bendravimu su atakuojamuoju asmeniu arba siekiu manipuliuoti atakuojamojo asmens veiksmais, pasinaudojus jo jausmais. Naudodami socialinės inžinerijos technologijas, kibernetiniai nusikaltėliai siekia savo užsibrėžtų tikslų. Pažymėtina, kad socialinės inžinerijos technologijos naudojamos ne tik tam, kad paveiktų asmenų nuomonę apie elektroninius rinkimus, bet ir tam, kad atliktų technologines elektroninių balsavimo sistemų atakas, siekiant sužlugdyti šių sistemų veikimą, įdiegiant sistemose kenkėjišką programinę įrangą.

Prie socialinės inžinerijos atakų gali būti priskiriami:

- *Kibernetiniai sukčiavimai* (*angl. Cyber fraud*), kurių kategorijai gali būti priskiriami tokie atakos metodai kaip: *fišingas* (*phishing*); *whailingas* (*angl. whaling*) ir kt., kurių pagrindinis tikslas yra „priversti“ asmenį savanoriškai atlikti tam tikrus kibernetiniam nusikaltėliui palankius veiksmus: nesąmoningai įdiegti kenkėjišką programinę įrangą, perduoti prisijungimo duomenis ar atlikti kitokius veiksmus, kurie sudarys piktavaliui palankias sąlygas įvykdyti tolimesnę jo planuojamą ataką;
- Valstybės *piliečių nuomonės formavimas*, siekiant sumenkinti elektroninių balsavimo sistemų įvaizdį. Dažnai elektroninės balsavimo sistemos yra pristatomos kaip įrankis, kuris yra nesaugus naudoti dėl jame naudojamų informacinių technologijų ir jų pažeidžiamumo. Pastovūs neigiami elektroninio balsavimo sistemų apibūdinimai ir informaciniai pranešimai, kuriose tvirtinama, kad toks balsavimo būdas yra nesaugus ir naudojamas tik tam, kad būtų suklastoti rinkimų rezultatai arba palengvinta balsų pirkimo galimybė, neabejotinai sumažins piliečių pasitikėjimą šiuo balsavimo būdu. Labai dažnai piliečių nuomonės formavimas yra grindžiamas asmens įsitikinimais ir prielaidomis, kad kibernetinio saugumo situacija yra kritinė, bet ne faktais;
- *Neigiamų faktų viešinimas*. Šis elektroninių balsavimo sistemų atakų metodas yra grindžiamas visuomenės poveikiu, paviešinant konkrečias elektroninių balsavimo sistemų spragas, kurios buvo aptiktos, atliekant įsibrovimus į šias sistemas;
- *Visuomenės klaidinimas*. Ši kibernetinė ataka vykdoma, siekiant suklaidinti piliečius ir priversti juos nepasitikėti elektroninėmis balsavimo sistemomis, paviešį-

nant niekuo nepagristą informaciją apie tai, kaip galimi elektroninio balsavimo vartotojai (rinkėjai) balsavo elektroninio balsavimo metu. Kibernetiniai nusikaltėliai, išanalizavę rinkėjų grupių charakteristikas, gali nesunkiai sudaryti tipinio rinkėjo, palaikančio tam tikrą politinį kandidatą, portretą bei prognozuoti jo polinkį naudotis elektroninių rinkimų sistemomis. Vienas iš būdų paveikti tokio rinkėjo norą naudotis elektroninių rinkimų sistemomis bei sumažinti pasitikėjimą šiomis sistemomis gali būti siejamas su netikros informacijos apie dalyvavusius rinkimuose ir jų išreikštą balsą paskelbimas. Jei tokia informacija viešumoje būtų paskelbta išankstinių internetinių rinkimų metu, galima tikėtis dalyvaujančiųjų pasyvumo padidėjimo ir balsavimo rezultatų pasikeitimų. Paskleista informaciją gali sukelti nepasitikėjimą internetiniais ir taip pat elektroniniais rinkimais.

Elektroninių balsavimo sistemų kibernetinių atakų metodai yra pavaizduoti 8 paveiksle.

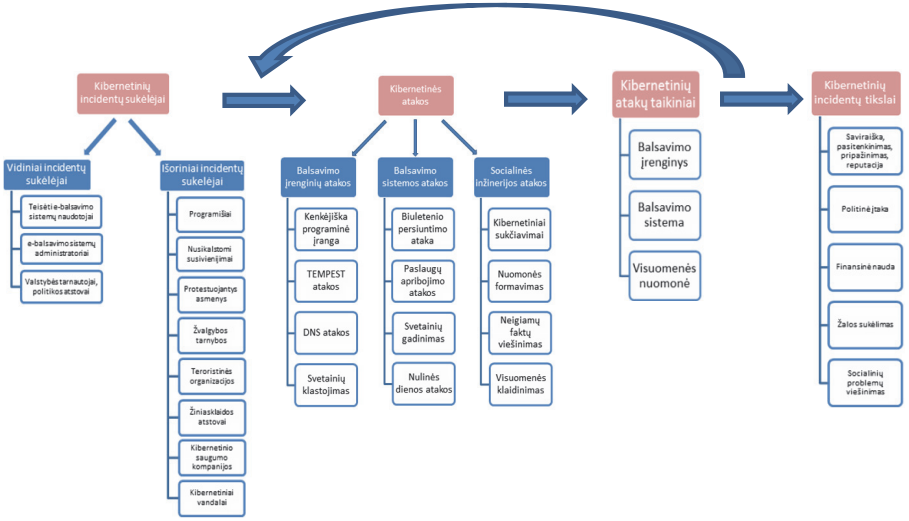


Šaltinis: *sudaryta autoriaus*

8 paveikslas. *Elektroninių balsavimo sistemų kibernetinių atakų metodai*

Apibendrinant galima teigti, kad kibernetinių incidentų sukėlėjai siekdami paveikti balsavimo sistemą, pasinaudos visomis įmanomomis galimybėmis ir visais įmanomais ir prieinamais įrankiais. Dažniausiai kibernetinė ataka neapsiriboja vienetiniu bandymu paveikti sistemą, o panaudojamas visas kompleksas kibernetinių atakų, kurios gali vykti nuosekliai arba lygiagrečiai tol, kol bus pasiektas kibernetinio nusikaltė-

lio užsibrėžtas tikslas. 9 paveiksle yra pateikta funkcinė schema, kurioje pavaizduotas kibernetinis incidentas elektroninių balsavimo sistemų kontekste.



Šaltinis: *sudaryta autoriaus*

9 paveikslas. *Kibernetinio incidento funkcinė schema*

Anksčiau įvardyti kibernetiniai incidentai apima ir technologines, ir žmogiškąsias grėsmes, kylančias elektroninio balsavimo sistemoms. Pasaulio mokslininkai ir kibernetinio saugumo ekspertai pažymi, kad didžiausias kibernetinis pažeidžiamumas yra susijęs su žmogiškuoju faktoriumi, kuris yra sunkiai nusakomas. Labai dažnai piktavališkų tikslų turintys asmenys, panaudodami socialinės inžinerijos technologijas ir metodus, siekia visais įmanomais būdais įtikinti atakos „auką“ atlikti tam tikrus veiksmus (Lackram, Padayachee, 2018). Nusikaltėliai „priverčia“ informacinių išteklių valdytojus ar naudotojus savanoriškai įdiegti kenkėjišką programinę įrangą jų valdomose sistemose (sistemos gali būti sujungtos į internetinius kompiuterinius tinklus arba neturėti išorinio ryšio). Tokiu būdu sutrikdomas normalus sistemų darbas, gadinami sistemoje saugomi duomenys arba kitaip trikdoma informacinių išteklių veikla. Toks socialinės inžinerijos technologijų panaudojimas ir kenkėjiškos programinės įrangos uždarose sistemose (artilerijos sistemos) įdiegimas buvo įvykdytas Ukrainoje 2014 metais. Šios atakos padariniai yra ypač dideli, kadangi jos pagrindinis tikslas buvo ne noras pakenkti ar destabilizuoti informacinių išteklių veiklą, bet kinetiškai paveikti artilerijos sistemas. Šis įvykis yra siejamas su Fancy Bear kibernetinių nusikaltėlių grupuote, kuri, kaip manoma, yra finansuojama žvalgybos tarnybų (Crowdstrike, 2017).

2. KONCEPTUALAUS KIBERNETINIO SAUGUMO VALDYMO MODELIO ELEKTRONINIAMS RINKIMAMS ĮGYVENDINTI STRUKTŪROS KŪRIMAS IR TYRIMO METODOLOGIJA

Ši disertacinio darbo dalis bus skirta kibernetinio saugumo valdymo modelio, kuris gali būti panaudojamas įgyvendinant elektroninius rinkimus, pradinės struktūros kūrimui bei įvertinimui, kuris bus atliekamas, pasinaudojant empiriniu tyrimu, kurio metu bus apklausiami kibernetinio saugumo ekspertai, o jų nuomonės ir atsakymai bus panaudoti, nustatant šio modelio tinkamumą kibernetinio saugumo valdymui užtikrinti organizacijoje, bei siūlomo kibernetinio saugumo valdymo modelio struktūrai tobulinti. Šioje dalyje taip pat yra analizuojami, mokslininkų atlikti teoriniai ir praktiniai tyrimai, susiję su kibernetinių incidentų ir pažeidžiamumų atsiradimu elektroninėse ir internetinėse balsavimo sistemose, taip pat žinomi išpuoliai, įvykdyti prieš elektronines rinkimų sistemas.

Pirmajame šios dalies poskyryje aprašomos kibernetinės atakos prieš pasaulio elektroninių rinkimų sistemas. Antrasis poskyris nagrinėja kibernetinio saugumo valdymo modelio kūrimo prielaidas bei principus, taip pat pateikia numatoma kibernetinio saugumo valdymo modelio struktūrą. Trečiajame ir ketvirtajame poskyryje yra pateikiama kibernetinio saugumo valdymo modelio tyrimo metodika, panaudota empirinio tyrimo organizavimo metu.

Pažymėtina, kad disertacinio darbo tikslas nėra siejamas su technologinių sprendimų priemonių parinkimu, siekiant užtikrinti kibernetinio saugumo valdymą organizacijoje. Mokslinėje literatūroje, teisės aktuose ir kituose šaltiniuose dažnai yra akcentuojamas technologinis neutralumas, o ypač – kritinės infrastruktūros ir kibernetinio saugumo sprendimų technologinis neutralumas (Marcinauskaitė, 2013; LRS, 2014; Papadaki, 2018; Huawei, 2019; Meltzer, 2020). Būtent dėl šios priežasties konstruojamas kibernetinio saugumo valdymo modelis yra technologiškai neutralus, o kiekviena organizacija (valstybė), nusprendusi naudoti šį modelį savo elektroninių rinkimų įgyvendinimo veikloje, gali pasirinkti, kokias technologines kibernetinio saugumo veiklos užtikrinimo priemones bei metodikas naudos, įgyvendindama šį modelį.

2.1. Kibernetiniai išpuoliai prieš pasaulio elektroninių rinkimų sistemas

Daugelis pasaulio demokratinių šalių naudojasi elektroninėmis balsavimo sistemomis: kai kurios šalys naudoja elektroninius įrenginius balsavimo apylinkėse, kitos vykdo elektroninius balsavimus, pasinaudodamos interneto tinklais. Tačiau pažymėtina, kad praktiškai visais elektroninio balsavimo sistemų panaudojimo atvejais nepriklausomų saugumo ekspertų atlikti balsavimo sistemų pažeidžiamumų tyrimai ir analizes parodė, kad sistemos turi savyje saugumo spragų ir pažeidžiamumų, kurie gali būti išnaudojami kibernetinių incidentų sukėlėjų, ir gali tapti rimta galimybe kibernetiniams nusikaltėliams sutrikdyti rinkimus, kompromituoti rinkimų rezultatus

arba atskleisti rinkėjų pareikštų balsų slaptumą. Šiame disertacinio darbo skyriuje bus pateikiami įvykdytų elektroninių balsavimo sistemų pažeidžiamumų tyrimų rezultatai ir bandoma paaiškinti, kodėl realiose elektroninio balsavimo sistemose aptiktos saugumo spragos yra taip plačiai paplitusios. Šiame skyriuje nagrinėjami elektroninių balsavimo sistemų pažeidžiamumai bus suskirstyti į elektroninių balsavimo įrenginių (elektroninių balsadėžių) ir internetinių balsavimo sistemų pažeidžiamumus.

Kaip jau buvo minėta anksčiau, elektroninės balsavimo sistemos gali būti atakuojamos, o asmenų, norinčių paveikti balsavimo sistemų veikimą, yra daug daugiau nei tradicinių rinkimų kontekste: tai ir balsavimo sistemas aptarnaujantis personalas, nesąžiningi politiniai veikėjai ir jiems dirbantys kibernetiniai nusikaltėliai, nedraugiškos valstybės, visuomenės iniciatyvinės grupės ir kt. Visų kibernetinių incidentų sukėlėjų grupių veiksmai, siekiant paveikti elektronines balsavimo sistemas, gali būti suskirstomi į tris poveikio balsavimo sistemai kategorijas:

1. elektroninių balsavimo rezultatų nustatymas ir prognozavimas (noras išsiaiškinti visuomenės balsavimo tendencijas; suprasti tam tikrų visuomenės sluoksnių tam tikro kandidato palaikymą);
2. elektroninių balsavimų rezultatų klastojimas (noras pakeisti rezultatus ir išrinkti tinkamą kandidatą);
3. elektroninių rinkimų proceso trikdymas arba diskreditavimas (noras technologiškai paveikti rinkimų sistemas, siekiant apriboti naudojimąsi sistemomis, akivaizdus rezultatų klastojimas arba melagingas pranešimas apie tokias veiklas).

Apginti elektronines balsavimo sistemas nuo įsibrovimų ir sumažinti saugumo pažeidžiamumų kiekį šiose sistemose yra ganėtinai sunku. Elektroninio balsavimo sistemos ir jų komponentai dažnai yra traktuojami ir gaminami kaip komerciniai įrenginiai arba komercinė programinė įranga. Toks požiūris yra iš esmės klaidingas (Dykstra, 2012; Halderman, 2017). Visi šie įrenginiai ir programinė įranga turi būti pozicionuojami kaip kritinės infrastruktūros (kritinių informacinių išteklių) dalis, o jų apsaugai ir saugumui turi būti skiriamas ypatingas dėmesys.

Pažymėtina, kad tam tikri saugumo mechanizmai bei technologijų naudojimas, diegiant ir projektuojant elektroninio balsavimo sistemas, gali apsaugoti jas nuo kylančių grėsmių, tačiau yra būtina atlikti nepriklausomus techninės ir programinės įrangos saugumo auditus, pasitelkiant ne tik vidinius, bet ir išorinius resursus.

Kaip pažymi J. Halderman, didžiausia problema, su kuria susiduria mokslininkai ir saugumo technologijų specialistai, vykdydami elektroninių balsavimo sistemų pažeidžiamumų tyrimus, yra siejama su šių sistemų uždarumu. Elektroninio balsavimo sistemų kūrėjai ir įrangos gamintojai bei valstybės institucijos, atsakingos už sistemų kūrimą ir naudojimą, pasinaudodamos teisinėmis priemonėmis ir jiems suteiktais įgaliojimais, sukuria teisines kliūtis piliečiams ir ekspertams gauti teisėtą prieigą prie sistemos ir atlikti jos saugumo pažeidžiamumų analizę (Halderman, 2017). Pažymėtina, kad tai tyrėjams kelia pagrįstų abejonių, kad jie, vykdydami tyrimus, gali pažeisti įstatymus. Kita vertus, kibernetiniai nusikaltėliai, vykdydami savo veiklą, negalvoja apie įstatymus ir jų nesilaiko.

Toliau bus pateikiami kibernetinio saugumo pažeidžiamumų išnaudojimo pavyzdžiai, kurie aiškiai parodo, kad elektroninės balsavimo sistemos nėra tobulos, bet tai visiškai nereiškia, kad, atlikus tam tikrus papildomus darbus, jos negali būti naudojamos balsavimo procese.

2.1.1. Internetinio balsavimo sistemų pažeidžiamumai

Internetinis balsavimas, kaip ir bet kuri kita informacinė sistema, gali būti pažeidžiamas. Internetinės balsavimo sistemos pagal savo prigimtį negali būti laikomos saugiomis, kadangi šių sistemų techninė ir programinė įranga yra prijungta prie pasaulinio interneto tinklo, o balsavimo sistemos serveriai tampa potencialiais kibernetinių incidentų sukėlėjų taikiniais. Pagrindinės internetinio balsavimo sistemų grėsmės yra siejamos su:

1. sistemoje naudojamos programinės įrangos saugumo pažeidžiamumais, kadangi balsavimo sistemų programinė įranga yra kuriama komercinės įrangos pagrindu;
2. interneto aplikacijų architektūrinių sprendimų netobulumu, kadangi neteisingai įdiegtos aplikacijos (*angl. WEB application*) gali sąlygoti visos sistemos kompromitavimą;
3. pasauline prieiga prie internetinių balsavimo sistemų, kadangi būtent dėl šios priežasties sistemos gali būti atakuojamos iš bet kurio pasaulio taško (Papathanasiou, Germanos, 2019), o atakos tikslas gali būti ne pačios sistemos techninės įrangos gadinimas ar rinkimų rezultatų klastojimas, o sistemos teikiamų paslaugų apribojimas (Simons, 2010; Halderman, 2017).

Kaip jau buvo minėta anksčiau, dalis pasaulio šalių vykdė eksperimentinius balsavimus internetu, bet nė viena šalis pasaulyje nenaudoja internetinių rinkimų taip plačiai, kaip tai daro Estija. Savo internetinių rinkimų modelį Estija pradėjo naudoti per 2005 metų rinkimus ir tapo pirmąja pasaulio šalimi, kurios balsavimo sistemoje internetiniai rinkimai buvo pasiūlyti visos šalies gyventojams. Estijos internetinių rinkimų sistemą estai traktuoja kaip tam tikrą instrumentą, kurio jie gali didžiuotis, bet tarp Estijos politinių partijų kyla tam tikras nesutarimas dėl šios sistemos naudojimo.

2013 metais Estijos centro partija netgi kreipėsi į Europos žmogaus teisių teismą su prašymu įvertinti elektroninę balsavimo sistemą, naudotą 2011 metų parlamento rinkimuose. Centro partijos pirmininkas Priit Toobal savo spaudos konferencijoje pareiškė, kad „*Centro partijos įsitikinimais, dabartinis teisinis reguliavimas ir elektroninės balsavimo sistemos panaudojimas prieštarauja šalies konstitucijai, kadangi naudojama internetinė balsavimo sistema yra nesaugi, o naudojamos sistemos skaidrumo stoka kenkia rinkimų rezultatams, bei daro įtaką valstybės piliečių pasitikėjimui viešąja valdžia*“ (news.err.ee, 2013). Estijos vyriausioji rinkimų komisija nesutiko su partijos nuomone ir pareiškė, kad Estijos elektroninio balsavimo sistema yra saugi ir gali būti naudojama. Taip pat 2013 metais nevyriausybinė organizacija Sąžiningi rinkimai (*est. Ausad Valimised*), kurios nariai taip pat yra Centro partijos tarybos nariai, surengė informacinę kampaniją, kurios metu kritikavo internetinių rinkimų sistemą ir šešiasdešimt aštuoniuose Talino miesto vietose pakabino plakatus su užrašais: „Jie gali ištrinti tavo

balsą“, „Kiekvienas e. balsas gali tapti grėsme Estijos nepriklausomybei“ ir „Jie gali atiduoti tavo balsą tam, kam panorės“ (baltic-course.com, 2016).

Nors elektroniniai rinkimai oficialios Estijos valdžios ir yra laikomi saugiais, tačiau kritikos elektroninių balsavimo sistemos saugumui tikrai netrūksta (Lipma, 2011; Simons, 2011; Springall ir kt., 2014). Mokslininkai savo tyrimuose pažymėjo, kad Estijos elektroninė balsavimo sistema yra pažeidžiama ir įvardijo pagrindinius pažeidžiamumų aspektus:

- balsavimo slaptumo pažeidimo grėsmė;
- asmeninio balsavimo įrenginio (pvz., asmeninio kompiuterio naudojamo balsavimo metu) pažeidžiamumo grėsmė;
- vidinio įsibrovimo į balsavimo sistemą grėsmė;
- elektroninės balsavimo sistemos techninės ir programinės įrangos technologinės atakos;
- sistemos „uždarumo“ auditui ir saugumo patikrinimams problema.

Kompiuterinių sistemų saugumo ekspertai savo tyrimuose pažymi, kad Estijos elektroninių rinkimų sistemos saugumas yra labiau grindžiamas procedūrinėmis priemonėmis (taisyklėmis), o ne technologiniais sprendimais (Simons, 2011; Chowdhury, 2013; Springall ir kt., 2014; Halderman, 2017). Pasak mokslininkų, dabartinė kibernetinio saugumo situacija pasaulyje yra pasikeitusi, o nuo to laiko, kai Estijos internetinių rinkimų sistema pradėjo funkcionuoti, atsirado naujų kibernetinių grėsmių (pažeidžiamumų išnaudojimo metodai): kibernetiniai karai, kurie XX amžiaus pabaigoje buvo laikomi tik hipotetine grėsme, šiais laikais tapo aiškiai matoma ir suvokiama problema, o JAV karinė doktrina išskyrė penktąjį kariavimo domeną – informacinę (kibernetinę) erdvę (Economist, 2010). Kibernetiniai karai ir užsienio valstybių išpuoliai kibernetinėje erdvėje šiuolaikiniame pasaulyje tapo vienu iš didžiausių iššūkių, o realus bandymas paveikti elektronines balsavimo sistemas buvo fiksuotas per 2014 metų Ukrainos rinkimus (Halderman, 2017).

2014 metai mokslininkų grupė išspausdino tyrimą, kuriame aiškiai parodė, kokios saugumo spragos egzistuoja Estijos internetinio balsavimo sistemoje, bei pateikė šių spragų panaudojimo mechanizmus (Springall ir kt., 2014). Atlikdami tyrimą, mokslininkai stebėjo Estijos 2013 metų rinkimų eigą ir vykdomas procedūras, bendravo su sistemos administratoriais ir oficialiais valdytojas bei atliko technologinius programinės įrangos testus.

Atlikus tyrimus, buvo nustatyta, kad visos saugumo priemonės, naudojamos elektroninėje balsavimo sistemoje, gali būti pažeidžiamos, todėl balsavimo rezultatai gali būti neįskaitomi arba klastojami. Taip pat buvo pažymėta, kad balsavimo sistemos paruošiamieji darbai (programinės įrangos kūrimas ir atnaujinimas, programinės įrangos persiuntimas į balsavimo sistemą ir kt.) vykdomi, naudojant nesaugią infrastruktūrą (asmeninius kompiuterius), o tai gali būti priimtina tik informacinėse sistemose, kurios nėra kritinės. Mokslininkai rekomendavo nenaudoti Estijos internetinio balsavimo sistemos šalies rinkimuose, tačiau į šią rekomendaciją nebuvo atsižvelgta (Halderman, 2017).

Kitas internetinio balsavimo sistemos pažeidžiamumų išnaudojimo pavyzdys yra 2010 metais Wolchok ir kitų mokslininkų atliktas JAV Vašingtono internetinio bal-

savimo sistemos atsparumo pažeidžiamumams testas, kurio metu balsavimo sistema, kuri turėjo būti naudojama vyksiančiuose rinkimuose, buvo visiškai diskredituota (Wolchok, 2012). Balsavimo sistemos kūrėjai (valstijos valdžios atstovai) planavo panaudoti sistemą balsavimo procese. Siekdami įtikinti visuomenę sistemos saugumu ir išmokyti gyventojus naudotis sistema, suteikė visuomenei galimybę tris paras išbandyti sistemą bandomuosiuose balsavimuose, leido atlikti sistemos pažeidžiamumų paiešką ir vykdyti kibernetines atakas prieš sistemą be teisinių pasekmių. Mičigano universiteto mokslininkų komanda, vadovaujama A. J. Halderman, sugebėjo per trisdešimt šešias valandas nuo sistemos veikimo pradžios įvykdyti įsilaužimą į sistemą ir beveik perimti visišką sistemos kontrolę.

Tyrėjai, pasinaudodami balsavimo sistemos architektūros spragomis, netobulu techninės ir programinės įrangos konfigūravimu bei žmogiškosiomis klaidomis, parodė: jei sistema būtų atakuojama piktavalių, tai jie galėtų užsitikrinti prieigą prie balsavimo sistemos; pakeisti sistemoje esančius ir ateityje į ją pateksiančius piliečių balsus; kompromituoti balsavimo slaptumą; paslėpti įsibrovimo į sistemą pėdsakus (Wolchok, 2012; Halderman, 2017). Po šios mokslininkų įvykdytos „kibernetinės atakos“, rinkimų atstovai nusprendė nenaudoti šios internetinio balsavimo sistemos rinkimų metu.

Internetinio balsavimo sistemą taip pat buvo bandoma įdiegti daugiausiai gyventojų turinčioje Australijos Naujojoje Pietų Velso (*angl. New South Wales*) valstijoje. Šią sistemą buvo bandoma panaudoti per 2015 metų rinkimus, kuriose galėjo dalyvauti visi valstijos gyventojai, o sistemos panaudojimas internetinio balsavimo istorijoje yra pažymimas kaip daugiausiai naudotojų (rinkėjų) pritraukusi internetinio balsavimo sistema (Halderman, Teague, 2015), nors ja ir pasinaudojo tik penki procentai visų balsavimo teisę turinčių piliečių (balsavimo metu daugiau nei 280 tūkstančių balsų buvo gauti, pasinaudojant sistemos teikiamomis galimybėmis).

Australijos gyventojai, dalyvavę internetiniame balsavime, galėjo pareikšti savo nuomonę rinkimuose, pasinaudodami interneto svetainėmis, kurias administravo rinkimų komisijos specialistai, o pačią internetinio balsavimo sistemą sukūrė SCYTL kompanija. Kaip jau buvo minėta anksčiau, internetinių balsavimų sistemų techninės ir programinės įrangos tikslus aprašymas ir konfigūracijos dažniausiai nėra viešinamos, o nepriklausomi saugumo specialistai negali atlikti šių sistemų pažeidžiamumų patikrinimų. Panaši situacija buvo susiklosčiusi ir Australijoje, kai rinkimų komisija ne paviešino internetinės balsavimo sistemos išeigos kodų, bet pateikė visuomenei balsavimo sistemos veikimo principus (Brightwell1, 2014), o pati atliko saugumo pažeidžiamumų analizę (NSW Electoral Commission, 2014). Oficialių institucijų atlikti veiksmai, viešinant internetinio balsavimo sistemos veikimo principus bei atliekant saugumo pažeidžiamumų vertinimą, buvo nepakankami, kadangi pateiktos medžiagos apimtis ir turinys, pasak Halderman, negalėjo sudaryti sąlygų nepriklausomiems ekspertams iš esmės išnagrinėti sistemos saugumą (Halderman, 2017).

Nepriklausomi saugumo ekspertai, mokslininkai J. Halderman ir V. Teague, atliko sistemos pažeidžiamumų analizę internetinio balsavimo metu, o pats pažeidžiamumų testas buvo susijęs tik su tomis balsavimo sistemos dalimis, kurios buvo pasiekiamos viešai visiems balsuojantiems asmenims, testavimo metu nepažeidžiant įstatymų.

Testavimo metu buvo aptikti keli saugumo pažeidžiamumai: vienas iš pažeidžiamumų buvo susijęs su vartotojų naudojamos interneto naršymo programinės įrangos pažeidžiamumu; taip pat buvo pažeidžiama internetinės balsavimo sistemos programinė įranga (mokslininkai aptiko jau žinomas spragas, o taip pat nulinės dienos saugumo spragą) (Halderman, Teague, 2015; Halderman, 2017). Šio tyrimo metu mokslininkai parodė, kad internetinio balsavimo sistema yra pažeidžiama, o kibernetiniai nusikaltėliai gali pažeisti piliečių pateiktų balsų slaptumą, pakeisti piliečių balsus arba, pasinaudodami žmogaus viduje ataka, nubalsuoti taip, kaip nusikaltėliams yra palanku.

Po to, kai informacija apie internetinėje balsavimo sistemoje aptiktus pažeidžiamumus buvo perduota Australijos reagavimo į kompiuterinius incidentus komandai (*angl. Computer emergency response team (CERT)*), vienas iš pažeidžiamumų buvo panaikintas internetinio balsavimo sistemos naudojimo metu, tačiau, pažymėtina, kad iki tol sistemoje fiksuoti balsai nebuvo anuliuoti (Halderman, 2017).

Galima teigti, kad anksčiau išnagrinėti internetinių balsavimo sistemų pažeidžiamumų aptikimo ir praktinio išnaudojimo metodai parodo, kad šios sistemos bent jau kol kas nėra saugios, tačiau ateityje galima tikėtis, kad moksliniai tyrimai ir mokslininkų grupių kuriamos technologijos gali paversti šias sistemas naudojamomis kiekvienos šalies rinkimuose.

2.1.2. Elektroninio balsavimo įrenginių pažeidžiamumai

Nagrinėjant kibernetinį saugumą elektroninių rinkimų, vykdomų pasinaudojant elektroniniais balsavimo įrenginiais balsavimo apylinkėse, kontekste taip pat neabejotinai kyla klausimas, ar tokie balsavimo įrenginiai yra saugūs ir ar šių balsavimo įrenginių grupė neturi tam tikrų saugumo pažeidžiamumų, kurie gali būti išnaudojami, siekiant paveikti balsavimo rezultatus, kadangi tiesioginio balsavimo elektroniniai įrenginiai (elektroninės balsadėžės) yra tiesiog tam tikriems poreikiams modifikuoti (adaptuoti) kompiuteriai. Mokslininkai yra skeptiški šių įrenginių atžvilgiu, nes pasaulinė patirtis įrodo, kad programinė įranga (nepaisant programinės įrangos gamintojo) gali turėti pažeidžiamumų ir saugumo spragų, o kibernetinių nusikaltėlių noras paveikti tam tikrą programinę įrangą ir jos saugumo spragas priklauso tik nuo programinės įrangos paplitimo pasaulyje.

Elektroninės balsadėžės buvo panaudotos kelių pasaulio šalių rinkimuose: JAV, Brazilija, Nyderlandai ir kt. JAV elektroninės balsadėžės, kurias gamino „Diebold“ kompanija, buvo panaudotos per 2006 metų rinkimus. Šių balsadėžių programinės ir techninės įrangos sandara (architektūra ir programinės įrangos išeities kodai) nebuvo žinoma nepriklausomiems ekspertams, tačiau 2003 metais žmogiškosios klaidos metu buvo nutekintas pradinis programinės įrangos kodas (Jones, 2003), kurį nagrinėjo saugumo specialistai (Kohno, 2004; Hursti, 2006; Fieldman ir kt., 2006), o jų pateiktos išvados dėl programinės įrangos ir pačių įrenginių saugumo buvo vienareikšmiškos: buvo siūloma nenaudoti minėtų įrenginių rinkimų procesuose.

Nepriklausomų saugumo ekspertų ir mokslininkų komanda, vadovaujama A. Fieldman, patvirtino visus pažeidžiamumus, kuriuos kiti tyrėjai (Kohno, 2004; Hursti, 2006) aptiko „Diebold“ elektroninėse balsadėžėse, taip pat praktiškai parodė, kaip

galima išnaudoti pažeidžiamumus ir manipuliuoti elektroniniais balsais, kurios rinkėjai pateikė balsavimo metu. Mokslininkai taip pat atrado, išnagrinėjo ir paviešino sistemos pažeidžiamumus, kurie iki tol nebuvo žinomi (Fieldman ir kt., 2006). Pagrindiniai tyrėjų grupės atlikto tyrimo rezultatai buvo susiję su balsavimo įrenginiuose aptiktais pažeidžiamumais, kurie suteikdavo galimybes:

1. piktavaliui, turinčiam fizinę prieigą prie balsavimo įrenginio arba prie laikmenos, iš kurios yra užkraunama balsadėžės programinė įranga (operacinė sistema), įdiegti kenkėjišką programinę įrangą į balsadėžę. Tyrėjai, aptikę šią spragą, patvirtino H. Hursti atliktą tyrimą ir patvirtino, kad balsadėžė gali būti „išmokinta“ vykdyti papildomas („nedokumentuotas“) funkcijas, pakeičiant jos atminties lustus arba modifikuojant jos valdymo programą (Hursti, 2006);
2. piktavaliui įdiegti rinkėjo balsų modifikavimo (vagystės) programinę įrangą į balsadėžę, o šios įrangos veikimas bus visiškai nepastebimas, nagrinėjant balsavimo įrenginio veikimo ataskaitas (*angl. logs*) ir vykdant balsadėžių auditavimo procedūras;
3. kibernetiniams nusikaltėliams įdiegti į balsadėžes kenkėjišką programinę įrangą (virusą), kuri gali savarankiškai plisti tarp balsadėžių pasiruošimo rinkimams ir pačių rinkimų metu, ir porinkiminėse fazėse, kuomet balsadėžės buvo aptarnaujamos techninio personalo balsavimus kontroliuojančioje įstaigoje (Fieldman ir kt., 2006).

Tyrimai, kurie buvo atlikti JAV, parodė, kad „Diebold“ elektroninės balsadėžės nėra saugios, tačiau, atlikdami tyrimus su kitų gamintojų balsavimo įrenginiais, mokslininkai ir saugumo ekspertai konstatavo, kad visi elektroninio balsavimo įrenginiai turi panašių pažeidžiamumų, o jų išnaudojimas galimas, kai yra galima fizinė prieiga prie įrenginio (Halderman, 2017). Pažymėtina, kad fizinės prieigos kontrolė ir fizinė įrenginių apsauga gali būti pasiekiama, pasinaudojant organizacinėmis saugumo priemonėmis (vidinėmis saugumo taisyklėmis ir kt.). Dauguma JAV valstijų, atsižvelgdamos į mokslininkų atliktų tyrimų rezultatus ir atskleistus pažeidžiamumus bei į materialinių išteklių elektroniniams balsavimo įrenginiams atnaujinti trūkumą, nusprendė atsisakyti elektroninių balsadėžių naudojimo, o 2014 metais apie septyniasdešimt procentų balsuojančių piliečių pareiškė savo nuomonę rinkimuose, pasinaudodami tradiciniais (popieriniais) balsavimo biuleteniais (ACM TechNews, 2014).

Nyderlandų karalystė savo rinkimų procesuose taip pat naudojo elektronines balsadėžes, kurias gamino olandiško kapitalo kompanija NEDAP. Olandijoje vykstančiuose rinkimuose elektroninės balsadėžes buvo naudojamos. Elektroninėse balsadėžėse buvo surenkama apie devyniasdešimt procentų visų dalyvaujančių rinkimuose asmenų balsų. Šių elektroninių įrenginių naudojimas buvo paplitęs visoje Olandijoje, tačiau ne visi piliečiai buvo patenkinti šios technologijos panaudojimu rinkiminiuose procesuose, o susikūrusi aktyviai besipriešinančių piliečių grupė kartu su mokslininkais R. Gonggrijp ir W. Hengeveld atliko balsadėžių pažeidžiamumų analizę ir savo išvadas pateikė visuomenei (Gonggrijp, Hengeveld, 2007).

R. Gonggrijp sukurta visuomeninė organizacija, pavadinimu „*Mes nepasitikime balsavimo kompiuteriais*“ (*oland. Wij vertrouwen stemcomputers niet*), per nacionalinę

televiziją pareiškė, kad jiems pavyko sėkmingai įsibrauti į NEDAP balsavimo kompiuterius. Organizacijos atstovai pademonstravo, kaip, atliekant nesudėtingus balsavimo kompiuterių techninės įrangos modifikavimo darbus (kompiuterinių mikroschemų pakeitimus), per vieną minutę galima paveikti elektroninę balsadėžę: priversti balsavimo įrenginį netiksliai įrašinėti balsavimo rezultatus arba „išmokinti" balsadėžę žaisti šachmatais (Gonggrijp, Hengeveld, 2007; Halderman, 2017). Pažymėtina, kad piktavaliai, kaip ir JAV „Diebold" kompanijos įrenginių atveju, turi turėti fizinę prieigą prie balsavimo įrenginio arba jo jungčių.

Olandijos atveju balsavimo įrenginių tyrimas taip pat atskleidė ir kitus pažeidžiamumus: lengvai atspėjamas įrenginio techninio konfigūravimo slaptažodis bei pažeidžiamumas, susijęs su dideliu elektromagnetiniu spinduliavimu, sklindančiu nuo elektroninių balsadėžių. R. Gonggrijp ir W. Hengeveld kartu su prieš elektroninius balsavimus nusiteikusia piliečių grupe atliko elektromagnetinio spinduliavimo (*angl. TEMPEST*) ataką ir, pasinaudodami elektromagnetinių bangų skeneriu ir dažnių analizės įrenginiu, pademonstravo, kaip galima iš dvidešimties metrų atstumo nustatyti, kaip balsavo rinkimuose dalyvavęs pilietis, pažeidžiant balsavimo slaptumo principą (Gonggrijp, Hengeveld, 2007; Limba, Agafonov, 2012; Halderman, 2017; Limba ir kt., 2017). Nyderlandų vyriausybė, siekdama apsisaugoti nuo galimų balsadėžių elektromagnetinių atakų, bandė modifikuoti NEDAP balsavimo įrenginius, pasinaudodama vienos iš Nyderlandų Karalystės kompanijų paslaugomis, ir apsaugoti įrenginius nuo TEMPEST tipo atakų. Po 2007 metų spalio mėnesio Amsterdamo teismo sprendimo panaikinti elektroninių balsadėžių sertifikavimą, Vyriausybė 2008 m. gegužės mėnesį nusprendė ateityje rengti rinkimus, kuriuose bus naudojami tik popieriniai balsavimo biuleteniai ir raudonos spalvos žymekliai, o idėjos apie elektroninių balsadėžių modernizavimą ir tolimesnį elektroninio balsavimo vystymą buvo atsisakyta (Stichting Wij Vertrouwen Stemcomputers Niet, 2008; Halderman, 2017).

Elektroninės balsavimo mašinos buvo naudojamos ne tik anksčiau paminėtose šalyse. Laikoma, kad anksčiausiai šią balsavimo technologiją pradėjo naudoti Brazilija, kurioje elektroniniai rinkimai vykdomi nuo 1996 metų Tuomet elektroniniais balsavimo įrenginiais pasinaudojo vienas trečdalis visų rinkimų teisę turinčių piliečių, o 2000 metais įvykę rinkimai buvo vykdomi tik su elektroninėmis balsadėžėmis (Filho, 2005; Superior Electoral Court, 2014). Ilgą laiką Brazilijoje naudojamų elektroninių balsavimo įrenginių saugumu buvo abejojama, tačiau Vyriausioji rinkimų komisija atmesdavo visus kaltinimus ir blokuodavo mokslininkų ir nepriklausomų saugumo ekspertų pastangas atlikti balsavimo įrenginių pažeidžiamumų analizę (Halderman, 2017).

Pirmasis Brazilijoje naudojamų elektroninių balsadėžių pažeidžiamumų testavimas buvo atliktas 2009 metais. Tais metais įrenginys buvo pateiktas mokslininkams ir saugumo ekspertams ir jiems buvo leista atlikti pažeidžiamumų paiešką. Tačiau mokslininkai neturėjo prieigos prie elektroninės balsadėžės architektūros ir programinės įrangos išeities kodų. Antrojo testavimo metu (2012 metais) įrenginiai buvo testuojami dar kartą, tačiau Brazilijos vyriausioji rinkimų komisija galėjo pasirinkti, kokios

testuotojų grupės galės dalyvauti renginyje, bei paruošė griežtas taisykles, reglamentuojančias testavime dalyvavusių grupių veiksmus. 2012 metų testavime dalyvavusi keturių mokslininkų komanda atliko balsavimo įrenginių pažeidžiamumų testavimą ir nustatė programinės ir techninės įrangos pažeidžiamumus (Aranha ir kt., 2014; Halderman, 2017), kurios pristatė savo moksliniame straipsnyje, bei pateikė rekomendacijas, kaip mažinti šiuos pažeidžiamumus. Mokslininkai identifikavo, kad:

- balsadėžėse netinkamai užtikrinamas balsavimo biuletenių slaptumas;
- balsavimo įrenginiuose netinkamai naudojami šifravimo algoritmai ir saugomi šifravimo raktai;
- balsavimo įrenginiai yra nepakankamai apsaugoti nuo vidinių saugumo incidentų sukėlėjų;
- elektroninių balsadėžių programinės įrangos architektūra ir panaudoti sprendimai sudaro galimybes įdiegti į balsadėžes kenkėjišką programinę įrangą;
- elektroninių balsadėžių atsparumas programinės įrangos pakitimams yra nepakankamas (Aranha ir kt., 2014).

Nors mokslininkai ir pateikė rekomendacijas bei identifikavo elektroninių balsadėžių pažeidžiamumus, Brazilijos vyriausioji rinkimų komisija ir toliau naudoja elektronines balsadėžes Brazilijos rinkimuose (Aranha ir kt., 2014; Superior Electoral Court, 2018)

Pažymėtina, kad elektroninių balsavimo sistemų naudojimas pasaulio šalių valdymo procesams įgyvendinti yra vienas iš pagrindinių klausimų šiuolaikinės visuomenės ir šiuolaikinės demokratijos kontekste. Be jokių abejonių galima teigti, kad elektroninės balsavimo sistemos turi pranašumų prieš tradiciniu būdu veikiančias sistemas: teisingai veikianti elektroninių balsavimų sistema suteikia saugumą, naudojimo patogumą, yra lengvai ir greitai aktyvuojama bei mažina rinkimų organizavimo kaštus. Visų šių pranašumų visuma ir daro elektronines balsavimo sistemas patraukliomis bei skatina pasaulio valstybes naudoti jas savo politinio valdymo procesuose. Tačiau šis patrauklumas sukelia ir nepatogumų. Elektroninio balsavimo sistemos projektavimo ir kūrimo procesas tampa sudėtingas, kadangi apima keletą mokslinių tyrimų sričių: ekonomiką, psichologiją, sociologiją, politikos, informacinių technologijų ir kibernetinio saugumo mokslus. Elektroninių balsavimų sistemos turi būti kuriamos, atsižvelgiant į visus visuomenės sluoksnius ir individus, bei turi suteikti vienodas galimybes visiems asmenims dalyvauti rinkiminiuose procesuose, neatsižvelgiant į piliečių įgytą išsilavinimą, turimą negalią ar įgytą kompiuterinį raštingumą. Kuriamos balsavimo sistemos turi atitikti skaidrumo, suprantamumo, teisiškumo, naudojimo patogumo (paprastumo) ir saugumo kriterijus, kurie garantuoja, kad valstybės sukurta elektroninio balsavimo sistema bus patraukli naudoti (bus pripažinta visuomenės), o ja priimti sprendimai bus legitimūs ir neginčijami (Limba, Agafonov, 2012; Limba, Agafonov, 2013; Karda ir kt., 2016).

Apibendrinant galima teigti, kad pasitikėjimas elektroninėmis balsavimo sistemomis ir elektronine demokratija yra susijęs su kiekvieno žmogaus vidiniais nusistatymais ir asmeniniu pasitikėjimu naudojamomis sistemomis (Brar, 2018), tačiau, tikėtina, kad viešumoje pateikta informacija apie balsavimo sistemos pažeidžiamumus tikrai

padidins skeptiškai nusiteikusių piliečių gretas. Konstruojant ir kuriant elektronines balsavimo sistemas, būtina nuo pat pradžių kritiškai vertinti sistemų architektūrą, naudojamos techninės ir programinės įrangos saugumą bei vykdyti nuolatinį sistemų pažeidžiamumų aptikimo ir grėsmių identifikavimo auditą, mokyti visuomenę naudotis elektroninėmis balsavimo sistemomis ir socialinio marketingo priemonėmis skatinti visuomenės pasitikėjimą elektroniniais rinkimais. Visuomenės pasitikėjimas elektroninio balsavimo sistemomis yra neapčiuopiama ir sunkiai sukuriama sistemos pridėtinė vertė, kurios praradimas gali sąlygoti visišką sukurtos ir jau naudojamos elektroninio balsavimo sistemos žlugimą (Limba, Agafonov, 2013).

Dėl aukščiau išvardintų priežasčių, siekiant saugių elektroninių rinkimų įgyvendinimo bei elektroninio balsavimo sistemų saugumo, yra būtina naudoti kibernetinio saugumo valdymo modelį, kuriame kibernetinio saugumo valdymas būtų nagrinėjamas kompleksiškai.

2.2. Prielaidos kibernetinio saugumo valdymo modeliui kurti

Pradinis kibernetinio saugumo valdymo modelis yra sukurtas, vadovaujantis pasaulinėje literatūroje išskiriamais kibernetinio saugumo valdymo teoriniais požiūriais, kurie apima technologinį, organizacinį ir fizinės saugos požiūrį į kibernetinio saugumo valdymą organizacijoje.

Modelio konstravimas yra atliktas, pasinaudojant amerikiečių sociologo T. Parsonso (*angl. T. Parsons*) dvidešimtajame amžiuje susistemintais struktūrinio funkcionalizmo principais, kurie buvo skirti bet kuriai veikiančiai sistemai apibūdinti:

- *tikslo siekimo principas*, numatantis, kad bet kokia sistema turi nusistatyti savo prioritetus ir jų įgyvendinimo eiliškumą;
- *adaptacijos principas*, kuris teigia, kad bet kuri veikianti sistema turi gauti išteklių iš ją supančios aplinkos ir sugebėti juos paskirstyti sistemos viduje;
- *integracijos mechanizmo sukūrimo principas*, numatantis, kad bet kokie sistemoje vykstantis procesai turi būti reguliuojami bei koordinuojami;
- *vertybinių standartų palaikymo principas*, kuris teigia, kad bet kokioje sistemoje turi egzistuoti sistemą sudarančių komponentų valdymo priemonių rinkinys, suderinantis jų veiklą ir tikslus su visos sistemos siekiamais tikslais (Cancian, 1972; VLE, 2012; Voroncov ir kt., 2019).

Pažymėtina, kad šių anksčiau paminėtų principų panaudojimas suteikia galimybę sukurti kibernetinio saugumo valdymo modelį, kuris savyje sujungia technologinius, socialinius, teisinio reglamentavimo, incidentų ir rizikų valdymo bei vadovavimo aspektus.

Mokslinėje literatūroje, nagrinėjančioje kibernetinio saugumo valdymą, yra susiduriama su dvejopu požiūriu į kibernetinį saugumą:

- pirmasis požiūris yra siejamas su technologinių priemonių ir įrankių analize, kurios metu siekiama rasti efektyviausius techninius sprendimus kibernetiniam saugumui užtikrinti;
- antrasis požiūris nagrinėja kibernetinio saugumo valdymo lygmenį, siekiant nustatyti ir įgyvendinti veiksmingą kibernetinio saugumo valdymo modelį,

užtikrinantį atsakingą organizacijos ir jos vykdomos veiklos procesų valdymą (Deighton, 2015; Latham & Watkins, 2016; Moschovitis, 2018).

Kaip ir buvo pažymėta anksčiau, technologinio kibernetinio saugumo užtikrinimas negali būti traktuojamas kaip pakankama priemonė, užtikrinanti kibernetinį saugumą organizacijoje. Technologinio kibernetinio saugumo priemonių panaudojimas organizacijoje gali tik pagerinti organizacijos bei jos valdomų informacinių sistemų ar infrastruktūros kibernetinį saugumą, tačiau tai visiškai negarantuoja visiško atsparumo kibernetinėms grėsmėms užtikrinimo. Dabartiniais laikais, kai kibernetinių grėsmių skaičius sparčiai auga, o kibernetinių atakų, kurias naudoja nusikaltėliai, metodai tampa vis įvairesni, būtina mąstyti apie sprendimus, kurie kompleksiškai nagrinėja visus organizacijos vykdomos veiklos procesus (Limba ir kt., 2017).

Siekiant sukurti efektyvų kibernetinio saugumo valdymą organizacijoje, siūlomas konceptualus kibernetinio saugumo valdymo modelis bus sudarytas iš šešių toliau išvardytų kibernetinio saugumo dimensijų. Kiekvienai dimensijai įgyvendinti yra būtina nustatyti unikalų įgyvendinimo priemonių rinkinį, kuriuo būtų galima pasiekti organizacijos kibernetinio saugumo valdymo sistemos supratimą ir evoliuciją. Išsamus kiekvienos kibernetinio saugumo valdymo modelio dimensijų validavimo klausimų sąrašas bus pateiktas lentelėse.

1. *Organizacijos valdymo procesai*. Nagrinėjant kibernetinio saugumo valdymo modelį, galima teigti, kad ši modelio dimensija yra svarbiausia organizacijoje, o nuo jos įgyvendinimo priklauso visos organizacijos požiūris į kibernetinį saugumą (Solms, Solms, 2009). Kiekvienos šiuolaikinės organizacijos lyderis (vadovas) turi aiškiai suvokti svarbiausius organizacijos kibernetinio saugumo tikslus (Kaplan, 2017; Moschovitis, 2018) bei suprasti, kad visuomet egzistuoja kibernetinio saugumo rizikos, kurios niekada nebus pašalintos iš organizacijos gyvenimo (DHS, 2012; Deighton, 2015; Dalziel, 2016; KPMG, 2016; Limba ir kt., 2017; Garret, 2018). Visi organizacijos vadovai ir nariai privalo suprasti, kad nėra galimybės visiškai išvengti kibernetinio saugumo pažeidžiamumų (incidentų), bet būtina imtis priemonių, kurios sumažins šių incidentų padarinius, o kibernetinis saugumas turi tapti *kertiniu akmeniu,* įgyvendinant organizacijos veiklos procesus ir naujus projektus, t. y. kiekvienas organizacijos planuojamas projektas ar veikla turi būti visapusiškai peržiūrima ir įvertinama per kibernetinio saugumo prizmę (Donaldson ir kt., 2015; Limba ir kt., 2017). Visapusiškas organizacijos kibernetinio saugumo suvokimas, kaip pagrindinio bet kurio projekto elemento, užtikrins organizacijos vykdomų projektų sėkmę ir padės taupyti pinigus ir kitus organizacijos veiklai būtinus išteklius (Latham & Watkins, 2016).

2 lentelė. *Organizacijos valdymo procesų dimensijos validavimas*

Organizacijos valdymo procesai
Organizacijos valdymo procesų dimensija yra susieta su trumpalaikiais ir ilgalaikiais organizacijos tikslais, organizacijos strategija, valdymu bei vadovavimu organizacijai. Kokia yra kibernetinio saugumo valdymo reiškinio įtaka organizacijos valdymo procesų dimensijai?
Ar kibernetinio saugumo valdymo reiškinio suvokimas (supratimas) ir naudojimas organizacijoje, jos valdymo sistemoje bei tarp organizacijos narių veikia pačios organizacijos kibernetinio saugumo užtikrinimo procesą?
Kaip kibernetinis saugumas turi būti suprantamas organizacijos kasdieniame gyvenime ir jos vykdomoje veikloje?
Kokia yra kibernetinio saugumo dedamosios reikšmė organizacijos vykdomuose (naujai įgyvendinamuose) projektuose ir kaip gali būti tobulinamas kibernetinio saugumo dedamosios įtraukimas į organizacijos vykdomą veiklą?
Ar, siekiant kibernetinio saugumo užtikrinimo įgyvendinimo organizacijoje, yra būtina atlikti organizacijos valdymo procesų peržiūrą ir koregavimą? Kokių veiksmų privalo imtis organizacija, siekdama patobulinti savo valdymo procesus kibernetinio saugumo reiškinio kontekste: • Organizacijos siekiamų tikslų identifikavimas; • Organizacijos veiklos pokyčių identifikavimas; • Organizacijos aplinkos ypatumų nustatymas; • Kibernetinio saugumo reiškinio integravimas į organizacijos veiklos procesus; • Kiti veiksmai.

Šaltinis: *sudaryta autoriaus*

2. *Teisinis reguliavimas*. Ši siūlomo kibernetinio saugumo valdymo modelio dimensija nagrinėja teisinį reguliavimą, teisės aktų reikalavimus ir teisinius veiksmus bei aspektus, kurie turi būti įgyvendinti organizacijoje, siekiančioje pritaikyti šiuolaikinį kibernetinį saugumą savo veiklos procesuose. Mokslininkai pažymi, kad kibernetinis saugumas yra labai specifinė veiklos rūšis, kuriai yra būtinas nuoseklus ir detalus teisinis reglamentavimas (Štitilis, 2013; Appazov, 2014; Limba ir kt. 2017; Kosseff, 2018). Pažymėtina, kad šioje dimensijoje turi būti nagrinėjami ne tik organizacijai ar jos veiklai taikomi išorinės aplinkos norminiai teisės aktai, bet ir vidinės aplinkos teisinis reglamentavimas, t. y. organizacijos parengtos taisyklės, reglamentuojančios darbuotojų, informacijos apsaugos pareigūnų, kompiuterinio tinklo administratorių veiklą ir atsakomybę (Deighton, 2015; Latham & Watkins, 2016; Brisch, 2017; Kosseff, 2018). Taip pat ši dimensija gali numatyti ir / ar aprašyti tam tikrus standartus, kurie naudojami arba planuojami naudoti ateityje organizacijos veikloje, įgyvendinant kibernetinio saugumo valdymą.

3 lentelė. *Teisinio reguliavimo dimensijos validavimas*

Teisinis reguliavimas
Kibernetinio saugumo valdymo modelio teisinio reguliavimo dimensija yra siejama su organizacijoje vykstančiais bei jai įtaką darančiais teisinio reglamentavimo procesais. Kokios priežastys lemia būtinybę nagrinėti teisinio reguliavimo organizacijoje sritį kibernetinio saugumo kontekste? Ar teisinio reguliavimo procesai organizacijoje gali turėti įtakos kibernetiniam saugumui organizacijoje?
Ar, nagrinėjant organizacijos kibernetinio saugumo valdymo įgyvendinimo kontekstą, būtina atsižvelgti į vidinės ir išorinės aplinkos teisinio reguliavimo poveikį organizacijai? Kokia organizacijos aplinka (išorinė ar vidinė), nagrinėjant ją kibernetinio saugumo teisinio reguliavimo kontekste, yra svarbesnė?
Kaip turi būti įgyvendinamas teisinis reguliavimas organizacijoje ir kokių veiksmų privalo imtis organizacija, siekdama patobulinti teisinio reguliavimo aspektus kibernetinio saugumo reiškinio kontekste: • Esamos teisinio reglamentavimo sistemos reikalavimų ir trūkumų nustatymas; • Trūkumų šalinimo priemonių įgyvendinimas; • Įgyvendintų priemonių taikymo organizacijos veikloje auditavimas; • Teisinio reguliavimo priemonių integravimas į organizacijos veiklos procesus; • Kiti veiksmai.

Šaltinis: *sudaryta autoriaus*

3. *Kibernetinio saugumo kultūra*. Ši kibernetinio saugumo dimensija yra sunkiausiai įgyvendinamas ir kontroliuojamas kibernetinio saugumo modelio aspektas, kuris būtinai turi būti integruotas į kibernetinio saugumo valdymo modelį. Organizacijose naudojamos technologinės kibernetinio saugumo priemonės, rizikos vertinimo ir valdymo technologijos, ekonominiai rizikos vertinimo rodikliai ir skaičiavimai gali suteikti žinių ir galimybių įvertinti, kas yra naudingiau organizacijai – įsigyti naują duomenų apsaugos sistemą ar priimti duomenų vagystės riziką, tačiau žymiai sunkiau yra įvertinti žmogiškojo faktoriaus įtaką kibernetiniam saugumui. Organizacija turi suprasti, kad jos pažeidžiamumas priklauso nuo organizacijos narių pažeidžiamumo (Solms ir Solms, 2009; Deighton, 2015; Štitilis, Klišauskas, 2015; Limba ir kt., 2017; Šarkūnas, 2017; James, 2018; Riddle, 2019). Kibernetinis saugumas turi būti suprantamas kiekvienam organizacijos nariui, o kiekvienas narys turi turėti galimybę išmokti ginti organizaciją ir save nuo kibernetinio saugumo incidentų (Singer, Friedman, 2014; WISAC, 2015; Limba ir kt., 2017), kadangi net menkiausia organizacijos nario klaida gali turėti įtakos visos organizacijos kibernetiniam saugumui ir veiklos procesams (Techrepublic, 2004; Wei ir kt., 2010; Trim, Lee, 2014; Deighton, 2015; Latham & Watkins, 2016). Viena iš didžiausių kibernetinio saugumo klaidų yra siejama su aukščiausio lygio vadovų ir informacinių technologijų specialistų noru turėti kuo daugiau privilegijų ir prieigos teisių prie naudojamų kompiuterinių sistemų (Trevors, Wallen, 2017; Haynes, 2019), bet, jeigu organizacija siekia visiško

kibernetinio saugumo, būtinas supratimas, kad visos saugumo priemonės turi būti taikomos visiems darbuotojams, kitaip kova dėl kibernetinio saugumo jau yra pralaimėta (Solms, Solms, 2009; Magklaras, Furnell, 2010; Trim, Lee, 2014; Šarkūnas, 2017; Caravelli, Jones, 2019).

4 lentelė. *Kibernetinio saugumo kultūros dimensijos validavimas*

Kibernetinio saugumo kultūra
Kibernetinio saugumo kultūros dimensija yra glaudžiai susijusi su žmogiškojo faktoriaus reiškinio įtaka kibernetinio saugumo valdymo procesui organizacijoje. Kokia yra pagrindinė kibernetinio saugumo kultūros problema organizacijos kibernetinio saugumo valdymo kontekste ir kokie galimi jos sprendimo būdai?
Ar organizacijos kibernetinio saugumo kultūros aspektai turi būti taikomi ir organizacijos partneriams bei organizacijai paslaugas teikiantiems partneriams?
Kokių veiksmų būtina imtis, organizacijoje sprendžiant žmogiškojo faktoriaus įtakos ir kibernetinio saugumo kultūros reiškinio problemas organizacijoje: • Identifikuoti kibernetinio saugumo suvokimo problematiką; • Numatyti kibernetinio saugumo suvokimo gerinimo metodus ir būdus; • Atlikti kibernetinio saugumo kultūros pokyčių stebėjimą; • Kiti veiksmai.

Šaltinis: *sudaryta autoriaus*

4. *Technologinis kibernetinis saugumas*. Kaip jau buvo minėta anksčiau, kibernetinis saugumas yra ne tik technologinis požiūris į organizacijos išteklių saugumą (Cayirci, Ghergherehchi, 2011; Solms, Niekerk, 2013; Campbell, 2017; Collier, 2018; Ernst & Young, 2018), bet kibernetinis saugumas negali būti užtikrinamas, nesinaudojant technologinėmis priemonėmis (Latham & Watkins, 2016; Limba ir kt., 2017; Walker, 2018). Ši kibernetinio saugumo valdymo modelio dimensija nagrinėja technologijas, kurios yra naudojamos organizacijoje. Organizacijos žinios apie technologinį kibernetinį saugumą ir jam užtikrinti panaudojamas priemones suteikia organizacijai galimybę suprasti, ar yra tam tikrų komponentų, kurie yra pažeidžiami ar gali būti pažeisti kibernetinio incidento metu, o technologinių apsaugos priemonių valdymas leidžia sumažinti laiką, kuris reikalingas kibernetinio saugumo incidento padariniams pašalinti arba užkirsti kelią kibernetinio saugumo incidento atsiradimui.

5 lentelė. *Technologinio kibernetinio saugumo dimensijos validavimas*

Technologinis kibernetinis saugumas
Technologinis kibernetinis saugumas dažniausiai siejamas su techninėmis ir programinėmis priemonėmis, kurios naudojamos kibernetiniam saugumui užtikrinti. Kokios dar technologinio kibernetinio saugumo įgyvendinimo priemonės yra svarbios, siekiant užtikrinti technologinį kibernetinį saugumą organizacijoje? Ar organizacijai yra būtina vadovautis tam tikrais technologinių priemonių valdymo standartais ar rekomendacijomis, siekiant darnaus technologinio kibernetinio saugumo vystymo? Ar technologinio kibernetinio saugumo valdymo priemonės turi turėti technologinį neutralumą? Nuo ko turi priklausyti technologinio kibernetinio saugumo užtikrinimo priemonių parinkimas organizacijoje? Kokius veiksmus privalo atlikti organizacija, siekdama užtikrinti tinkamą technologinio kibernetinio saugumo įgyvendinimą: • Naudojamų technologinių priemonių identifikavimas; • Technologinių priemonių parinkimas ir įdiegimas; • Technologinių priemonių panaudojimo įtakos kibernetiniam saugumui vertinimas; • Kiti veiksmai.

Šaltinis: *sudaryta autoriaus*

5. *Rizikos valdymas*. Modelio dimensija, nagrinėjanti organizacijos gebėjimą tinkamai identifikuoti aplinkos rizikas bei užtikrinanti, kad organizacija turi specialių įgūdžių, suteikiančių jai galimybes kontroliuoti šių rizikų poveikį organizacijos veiklos procesams. Kaip jau buvo minėta anksčiau, organizacija negali išvengti visų aplinkos pavojų ir rizikų, bet svarbu nustatyti visas galimas rizikas ir parengti veiksmų planą, kuris suteis galimybę sumažinti incidentų padarinius (Deighton, 2015; Latham & Watkins, 2016; Vega ir kt., 2017; Patiño ir kt., 2018). Vienas iš pagrindinių organizacijos gebėjimų yra ne tik išmokti vengti rizikų, bet mokėti jas valdyti (Solms ir Solms, 2009; Latham & Watkins, 2016; Limba ir kt., 2017; Walker, 2018). Pažymėtina, kad gebėjimas identifikuoti riziką ir parengti nenumatytų atvejų planus suteikia organizacijai daugiau pranašumo nei bandymas išvengti nustatytų rizikų.

6 lentelė. *Rizikos valdymo dimensijos validavimas*

Rizikos valdymas
Organizacijos rizikos valdymo procesas yra siejamas su organizacijos galimybėmis tinkamai identifikuoti, valdyti ir prisiimti jai iškylančias ir ją veikiančias vidinės ir išorinės aplinkos rizikas. Ar rizikos valdymo procesas yra svarbus organizacijai kibernetinio saugumo užtikrinimo kontekste? Ar kibernetinio saugumo valdymas organizacijoje gali būti vykdomas, neatsižvelgiant į rizikos valdymo aspektus? Kokių veiksmų turi imtis organizacija, siekdama tinkamai įgyvendinti rizikos valdymo procesus: • Identifikuoti rizikos valdymo procesus organizacijoje; • Suklasifikuoti galimas rizikas bei atlikti jų vertinimą; • Parengti rizikos valdymo planus ir taisykles; • Kiti veiksmai.

Šaltinis: *sudaryta autoriaus*

6. *Kibernetinių incidentų valdymas*. Ši dimensija yra glaudžiai susijusi su kibernetinio saugumo modelio teisinio reguliavimo dimensija, tačiau joje nagrinėjamos tik vykstančio arba jau įvykusio kibernetinio incidento valdymo taisyklės ir principai. Kibernetiniai incidentai ir jų valdymas yra labai komplikuotas procesas, nes jų atsiradimas ir aptikimas organizacijos valdomose informaciniuose ištekliuose yra visiškai nenuspėjamas ir gali būti tik hipotetiškai prognozuojamas (Craig, Valeriano, 2016). Organizacijai yra būtina turėti specialius planus ir taisykles, siekiant lokalizuoti vykstantį incidentą arba šalinant įvykusio incidento padarinius, nustatant visas priemones, kurios turi būti įgyvendintos, bandant sumažinti incidento poveikį ir atkurti normalią organizacijos veiklą (Deighton, 2015; Latham & Watkins, 2016; Limba ir kt., 2017; Walker, 2018).

7 lentelė. *Kibernetinių incidentų valdymo dimensijos validavimas*

Kibernetinių incidentų valdymas
Kibernetinių incidentų valdymas yra siejamas su organizacijos galimybėmis aptikti, suvaldyti bei efektyviai priešintis atsirandantiems ar vykstantiems kibernetiniams incidentams. Koks požiūris į kibernetinių incidentų valdymą yra labiau priimtinas šiuolaikiniame pasaulyje: atsako į kibernetinius incidentus (*angl. incident response*) ar kibernetinių incidentų valdymo (*angl. incident handling*)? Kokie šių požiūrių privalumai ar trūkumai gali būti identifikuojami kibernetinio saugumo valdymo organizacijoje kontekste? Ar, siekiant visapusiško kibernetinio saugumo organizacijoje, šie požiūriai į kibernetinių incidentų valdymą turi būti nagrinėjami neatsiejamai vienas nuo kito? Kokių veiksmų turi imtis organizacija, siekdama tinkamai įgyvendinti kibernetinių incidentų valdymą: • Reglamentuoti kibernetinių incidentų valdymo etapus; • Parengti organizacijos veiklos planus; • Atlikti įvykusių incidentų tyrimus, nustatant jų atsiradimo priežastis; • Kiti veiksmai.

Šaltinis: *sudaryta autoriaus*

Pažymėtina, kad aukščiau esančiose lentelėse pateikti kibernetinio saugumo valdymo modelio dimensijų validavimo klausimai buvo panaudoti atliekant empirinį tyrimą ir pateikiant juos ekspertams pradiniame tyrimo etape (plačiau žr. Tyrimo metodika).

Apibendrinta konceptualaus kibernetinio saugumo valdymo modelio struktūrinė schema yra pateikta 10 paveiksle, kuriame yra pavaizduojamos šešios kibernetinio saugumo valdymo dimensijos, kurių įgyvendinimas organizacijoje gali užtikrinti teorinį kibernetinio saugumo valdymą. Būtina pažymėti, kad visapusiškas kibernetinio saugumo įgyvendinimas bet kurioje organizacijoje turi būti suprantamas kaip tam tikras ciklinis veiklos procesas, kuris turi tapti nuolatiniu organizacijos veiklos procesu.

Atkreiptinas dėmesys, kad visos šešios kibernetinio saugumo valdymo modelio dimensijos turi būti įgyvendinamos vienu metu visoje organizacijoje (jos struktūriniuose padaliniuose), nes tik vienos ar kelių dimensijų įgyvendinimas neleis užtikrinti kibernetinio saugumo valdymo situacijos pagerinimo bei nesuteiks apčiuopiamos naudos organizacijos kibernetiniam saugumui.

Šaltinis: *Limba, Agafonov ir kt., 2017.*

10 paveikslas. *Kibernetinio saugumo valdymo modelis elektroninių rinkimų įgyvendinimui*

2.3. Tyrimo metodika

Planuojant kibernetinio saugumo valdymo modelio elektroninių rinkimų įgyvendinimui empirinį tyrimą, disertacinio darbo autorius susidūrė su problema, susijusia su tiriamojo reiškinio specifiškumu bei jo suvokimu visuomenėje. Būtent tiriamojo reiškinio specifiškumas ir nesuprantamumas visuomenėje ir suponuoja empirinio tyrimo metodo pasirinkimą. Neįmanoma nesutikti su nuomone, kad siekiant visapusiškai išnagrinėti vieno ar kito reiškinio probleminius aspektus, reikia taikyti kokybinius ir kiekybinius tyrimo metodus, kurie vienas kitą *papildo, kompensuoja*, tačiau dėl tam tikrų tiriamų dalykų specifiškumo kiekybinio ir kokybinio tyrimo tarpusavio derinimas ne visuomet yra įmanomas (Kardelis, 2016).

Atsižvelgiant į aukščiau išvardintas priežastis pasirenkant tyrimo metodiką buvo nuspęsta atlikti tik kokybinį tyrimą. Toks pasirinkimas yra sąlygotas aiškiu kibernetinio saugumo srities specifiškumo suvokimu: kokybinio tyrimo pasirinkimą lėmė ne tik tai, kad kibernetinis saugumas yra labai specifinė, daug specializuotų žinių reikalaujanti sritis, kuri dažniausiai mažai suprantama eiliniam piliečiui, bet ir tai, kad būtent šių žinių trūkumas sąlygos duomenų nepakankamumo problemos atsiradimą. Dėl šios priežasties atsiras prielaidos abejoti tyrimo rezultatų patikimumu.

Mokslininkai Burn ir Grove kokybinį tyrimą apibudino kaip *telkimąsi į žmogiškąsias patirtis, remiantis sisteminėmis ir sąveikomis grįstomis nuostatomis*, o patys kokybiniai tyrimai yra taikomi kai tyrimo tema yra mažai ištyrinėta (Žydžiūnaitė, Sabaliauskas, 2017). Kokybinių tyrimų metodai yra lankstus bei orientuoti į interpretaciją, o *taikomais metodais labiau gilinamasi į daiktų ir reiškinių kilmę, o ne į skaičių, kiekį,* (Kardelis, 2016), tokiu būdu kokybiniai tyrimai išryškiną reikšmes, sąvokas, apibrėžimus, savybes, metaforas, simbolius ir aprašymus (Lune, Berg, 2017; Shkedi, 2019). Būtina pažymėti, kad būtent dėl to, kad atliekant kokybinius tyrimus paprastai tiriamųjų reiškinių kokybė vertinama naudojant žodžius, vaizdus ir aprašymus, o dauguma kiekybinių tyrimų daugiausia remiasi skaičiavimais, atliekamais kompiuteriais, daugelis klaidingai mano, kad kiekybiniai tyrimai yra labiau vertingi moksline prasme, nei kokybiniai. Norint atlikti gerą kokybinį tyrimą, tyrėjas turi nueiti ilgą ir sunkų kelią, kurio vienoje pusėje yra sunkiai pasiekiami duomenys, kitoje labai griežti analizės reikalavimai (Lune, Berg, 2017). Taip pat pažymėtina, kad kokybiškas tyrimas reikalauja atitinkamos tyrėjo kvalifikacijos ir turimų žinių derinio. Kokybiniai tyrimai yra grindžiami *tyrėjo kaip instrumento* principu, kuriuo siekiama panaudoti tyrėjo turimas žinias, intuityvius, analitinius ir kitus sugebėjimus, (Žydžiūnaitė, Sabaliauskas, 2017; Lune, Berg, 2017; Shkedi, 2019).

Atkreiptinas dėmesys, kad kokybiniams kaip ir kiekybiniams tyrimams yra taikomi tam tikri patikimumo ir tinkamumo kriterijai. Siekiant užtikrinti atlikto kokybinio tyrimo patikimumą ir tinkamumą buvo vadovaujamasi mokslinėje literatūroje aptariamais tikrumo, perkeliamumo ir įtikinamumo principais (Žydžiūnaitė, Sabaliauskas, 2017).

Disertaciniame darbe atlikto kokybinio tyrimo tikslas yra įvertinti ne technologines saugumo priemones, naudojamas kibernetinio saugumo užtikrinimui, o nustatyti siūlomo konceptualaus kibernetinio saugumo valdymo modelio gyvybiškumą, bei gauti

specifines žinias turinčių ekspertų patarimus ir nuomones, siekiant modifikuoti konceptualaus modelio struktūrą ir padidinti jo įdiegimo galimybes.

Mokslinėje literatūroje yra aprašoma daugybė tyrimo proceso suskirstymo į etapus būdų ir metodų. Šiame disertaciniame darbe bus naudojamas Alano Braimano (*angl. Alan Bryman*) kokybinių tyrimų atlikimo (Bryman, 2001) modelis, kuris adaptuotas pagal A. Augustinaičio ir kitų mokslininkų siūlomą ekspertinio vertinimo procedūrą (Augustinaitis ir kt., 2009). Pažymėtina, kad atliekamas kokybinis tyrimas g*rindžiamas skerspjūvio nuostata*, kuomet apimamas tik vienas empirinis ciklas (Žydžiūnaitė, Sabaliauskas, 2017). Disertaciniame darbe atliktas empirinis tyrimas bus vykdomas septyniais etapais:

1. *Teorinių įžvalgų formavimo etapas*, apimantis mokslinės problemos formulavimą, tyrimo tikslų ir uždavinių nustatymą ir jų apibrėžimą;
2. *Tyrimo eigos sudarymo etapas*, kurio metu yra parengiami tyrimui reikalingi dokumentai, numatomas tyrimo metodas, vertinimo kriterijai bei tyrimo apribojimai;
3. *Ekspertų atrankos etapas*, kurio metu yra atliekamas ekspertų parinkimas, atsižvelgiant į jų turimas kompetencijas, žinias bei darbo konkrečioje tiriamoje srityje patirtį;
4. *Duomenų surinkimo etapas*, kurio metu yra surenkami tyrimo duomenys (gaunama informacija) iš tyrime dalyvaujančių ekspertų;
5. *Duomenų analizės etapas*, apimantis gautų duomenų analizę, galimų klaidų ir prieštaravimų pašalinimą;
6. *Rezultatų interpretavimo etapas*, apimantis tyrimo metu gautų rezultatų apibendrinimą bei bendros ekspertų nuomonės apie tyrimo objektą suformavimą;
7. *Rezultatų ir išvadų pateikimo etapas*, kurio metu yra pateikiamos oficialios atlikto tyrimo išvados ir rezultatai.

Empirinio tyrimo struktūrinė schema yra pateikta 11 paveiksle.

Šaltinis: *parengta autoriaus pagal Bryman, Augustinaitį ir kt.*

11 paveikslas. *Empirinio tyrimo struktūrinė schema*

Pažymėtina, kad, siekiant kuo tiksliau įvertinti ekspertinio tyrimo rezultatus ir teisingai interpretuoti ekspertų atsakymus, ekspertinis vertinimas buvo atliekamas dviem etapais: pirminiame etape ekspertams elektroniniu paštu buvo pateiktas struktūrizuotas klausimynas (kibernetinio saugumo dimensijų validavimo klausimai) ir buvo prašoma pateikti kiek įmanoma išsamesnius atsakymus; antro etapo metu (gavus atsakymus elektroniniu paštu) su ekspertais buvo bendraujama asmeninio susitikimo metu arba telefonu, siekiant maksimaliai tiksliai suprasti ekspertų nuomonę tam tikru klausimu ir aptarti bei patikslinti rašytine forma pateiktus ekspertų atsakymus. Disertacijos autoriaus nuomone, tokia ekspertinio vertinimo vykdymo procedūra suteikia daug geresnę galimybę tinkamai interpretuoti pateiktus rašytinius atsakymus, tačiau reikalauja papildomų laiko sąnaudų ir gilesnės pateiktų atsakymų analizės.

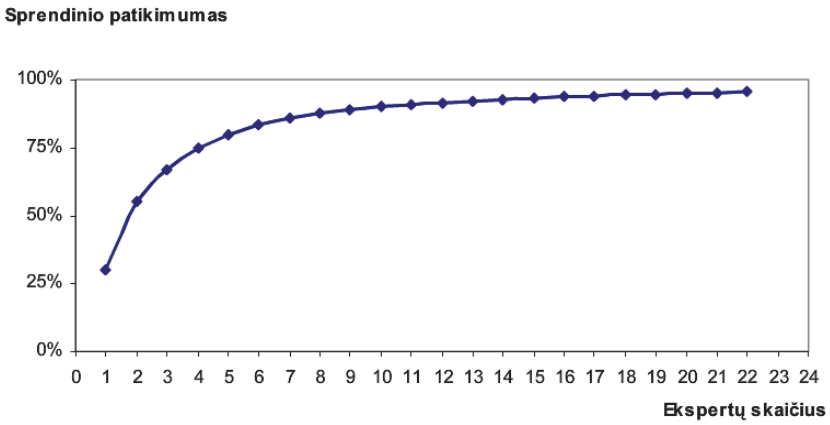
2.4. Ekspertų atranka ir jų savybės

Renkantis kibernetinio saugumo valdymo modelio empirinio tyrimo atlikimo metodą, buvo nuspręsta pasinaudoti ekspertinio vertinimo metodu, kadangi disertaciniame darbe nagrinėjama kibernetinio saugumo valdymo tema yra gana specifinė ir

reikalaujanti tam tikrų, ne tik technologinių žinių, bet ir bendro kibernetinio saugumo dalyko specifikos supratimo ir ekspertiškumo.

Ekspertinio vertinimo metodo parinkimą nulėmė disertacinio darbo autoriaus tikslas gauti ne panoraminį tyrime įvardijamos problemos vaizdą, bet konkrečios populiacijos tipinės grupės problemos suvokimą ir matymą, nes tik taip galima sudaryti tikslesnę ir konkretesnę specifinio reiškinio charakteristiką. Siekiant išvengti siauro, vien tik technologijomis grindžiamo požiūrio į kibernetinį saugumą, tyrimo imties sudarymo metu buvo pasirenkami ekspertai, kurių žinios ir patirtis kibernetinio saugumo srityje yra siejama ne tik su technologinių apsaugos priemonių panaudojimu kibernetinio saugumo užtikrinimo kontekste, bet ir su kibernetinio saugumo politikos gairių nustatymu, teisiniu reglamentavimu bei strateginio kibernetinio saugumo planavimu ir vystymu, kibernetinių saugumo incidentų rizikų valdymo procesu, elektroninių rinkimų sistemų atakų bei kritines infrastruktūros apsaugos priemonių organizavimu ir vertinimu. Toks ekspertų parinkimo metodas užtikrina, kad pasirinkti ekspertai bus susipažinę ne tik su technologinės kibernetinio saugumo problemos sprendimo būdais, bet suvoks ir turės patirties kitose kibernetinio saugumo užtikrinimo srityse. Šios anksčiau išvardytos ekspertų kompetencijos ir praktinio darbo kibernetinio saugumo srityje patirtis leidžia manyti, kad atlikto ekspertinio tyrimo rezultatai bus patikimi ir išsamūs, o visos ekspertų grupės apklausos rezultatai patvirtins kuriamo kibernetinio saugumo valdymo modelio gyvybiškumą ir praktinį pritaikomumą.

Sudarant ekspertinio tyrimo imtį, buvo vadovaujamasi metodologinėmis prielaidomis, suformuluotomis klasikinėje testų teorijoje, kurioje teigiama kad agreguotų sprendimų patikimumą ir ekspertų skaičių sieja greitai gęstantis netiesinis ryšis (Augustinaitis ir kt., 2009; Baležentis, Žalimaitė, 2011) (žr. 12 paveikslą).



Šaltinis: *Augustinaitis ir kt. (2009)*

12 paveikslas. *Ekspertų skaičiaus įtaka vertinimo patikimumui*

Pažymėtina, kad, vadovaujantis anksčiau pateiktu paveikslu, A. Augustinaičio ir kitų mokslininkų pateikiama nuomone, nedidelės ekspertų grupės sprendimų ir vertinimų

tikslumas apie tiriamą dalyką nenusileidžia didelės ekspertų grupės vertinimo tikslumui (Libby, Blashfield, 1978; Augustinaitis ir kt., 2009; Baležentis, Žalimaitė, 2011). Augustinaičio ir kitų mokslininkų rekomenduojamas optimalus imties dydis, vykdant ekspertinius vertinimus, yra nuo penkių iki devynių ekspertų (Augustinaitis ir kt., 2009). Dėl šios priežasties, taip pat dėl tiriamojo dalyko specifiškumo, sudarant tyrimo imtį šiame disertaciniame darbe, buvo nuspręsta atlikti devynių kibernetinio saugumo srities ekspertų apklausą, pasinaudojant pusiau struktūrizuoto interviu metodu. Būtina pastebėti, kad kaip jau buvo minima anksčiau, disertacijos autoriaus pasirinktam kokybiniam tyrimui atlikti, nėra būtina sudaryti didelę imtį, o devynių ekspertų imties pasirinkimo pagrįstumą patvirtino ir tyrimo metu matomas gautų duomenų prisotinimas.

Empirinio tyrimo metu apklausiami kibernetinio saugumo ekspertai buvo parenkami vadovaujantis patogiosios imties principu, tačiau kiekvienas iš respondentų turi mažiausiai dešimties metų darbo patirties kibernetinio saugumo srityje. Pažymėtina, kad apklausti ekspertai turi ne tik specifinių kibernetinio saugumo sferos žinių, bet ir atstovauja skirtingiems sektoriams – tyrime dalyvavo ne tik viešojo sektoriaus atstovai, bet ir akademinės visuomenės nariai, taip pat Australijos bendrovės Heston MRO, vykdančios orlaivių remontą ir priežiūrą Australijos bei Azijos regione, Informacinių technologijų departamento vadovai ir specialistai, anksčiau dirbę įvairiose šalies viešojo sektoriaus institucijose. Tokia skirtinga ekspertų patirtis kibernetinio saugumo užtikrinimo srityje, taip pat ir geografinės padėties sąlygoti sociokultūriniai skirtumai leidžia teigti, kad atlikto empirinio tyrimo duomenys yra patikimi, o empirinio tyrimo metu gautos išvados gali būti plačiai naudojamos ne tik Lietuvoje, bet ir kitose pasaulio šalyse.

Dauguma iš apklaustų ekspertų (dirbančių Lietuvoje), kurie šiuo metu yra valstybinio sektoriaus atstovai, buvę valstybės tarnautojai, statutiniai pareigūnai, akademinės visuomenės nariai, yra prisidėję prie kibernetinio saugumo kūrimo Lietuvoje, valstybės kibernetinio saugumo politikos ir strategijos planavimo, išreiškė norą dalyvauti empiriniame tyrime anonimiškai, neatskleidžiant nei jų tapatybės, nei turimos patirties, nei buvusios ar dabartinės darbovietės. Dėl šios priežasties, o taip pat vadovaujantis respondentų teisės į privatumą principais ir tyrimų etikos principais (Kardelis, 2019; Žydžiūnaitė, Sabaliauskas, 2017), visiems ekspertams, dalyvavusiems empiriniame tyrime, buvo suteikti identifikatoriai. Ekspertinio vertinimo informacija yra pateikta toliau esančioje lentelėje (žr. 8 lentelę).

8 lentelė. *Ekspertų ir interviu informacija*

Eksperto identifikatorius	Interviu trukmė (min)	Interviu data
1E	34	2019-09-12
2E	38	2019-09-14
3E	51	2019-09-17
4E	39	2019-09-23
5E	45	2019-09-27
6E	40	2019-10-05
7E	108	2019-10-08
8E	92	2019-10-14
9E	42	2019-10-17

Šaltinis: *sudaryta autoriaus*

3. KIBERNETINIO SAUGUMO VALDYMO MODELIO ELEKTRONINIAMS RINKIMAMS ĮGYVENDINTI EMPIRINIO TYRIMO REZULTATŲ IR STRUKTŪROS ANALIZĖ

Ši disertacinio darbo dalis bus skirta siūlomo kibernetinio saugumo valdymo modelio tyrimo rezultatams aptarti ir apibendrinti. Atlikus siūlomo kibernetinio saugumo valdymo modelio empirinį tyrimą, tyrimo metu gauti rezultatai ir ekspertų siūlymai bus panaudoti, patikslinant kibernetinio saugumo valdymo modelį. Taip pat šioje dalyje bus atliekama patikslinto kibernetinio saugumo valdymo modelio, kuris gali būti panaudojamas, įgyvendinant saugius elektroninius rinkimus, struktūros analizė bei pateikiamos kibernetinio saugumo valdymo modelio dimensijų įgyvendinimo rekomendacijos, kuriant saugią elektroninių rinkimų sistemą Lietuvoje.

Siūlomo kibernetinio saugumo valdymo modelio empirinis tyrimas buvo padalintas į tris logines dalis: pirmosios dalies tikslas – išsiaiškinti ekspertų požiūrį į kibernetinio saugumo reiškinį bei išsiaiškinti, kaip kibernetinis saugumas yra suvokimas dabartiniu laikotarpiu; antrosios dalies klausimais buvo siekiama išsiaiškinti kibernetinio saugumo ekspertų požiūrį į siūlomą kibernetinio saugumo valdymo modelį bei gauti rekomendacijas, kurios galėtų patobulinti disertacijos autoriaus sukurtą kibernetinio saugumo valdymo modelį; trečioje tyrimo dalyje buvo užduodami klausimai apie siūlomo kibernetinio saugumo valdymo modelio tinkamumą elektroniniams rinkimams Lietuvoje įgyvendinti, taip pat siekiama išsiaiškinti, kokios organizacijos ar institucijos turi būti įtrauktos į elektroninių rinkimų įgyvendinimo procesą Lietuvoje.

Išsiaiškinus empiriniame tyrime dalyvavusių ekspertų nuomonę apie kibernetinio saugumo reiškinio suvokimą (apibrėžimą), ekspertams buvo pateikta glausta informacija apie sukurtą kibernetinio saugumo valdymo modelį (jo struktūrą, dimensijas), taip pat buvo užduoti klausimai, siekiant identifikuoti kibernetinio saugumo ekspertų nuomonę apie tam tikros dimensijos svarbą kibernetinio saugumo valdymo organizacijoje kontekste bei dimensijų įgyvendinimo priemonių panaudojimo tikslingumą. Pažymėtina, kad ekspertinio tyrimo metu ekspertų buvo prašoma ne tik įvertinti siūlomų kibernetinio saugumo valdymo modelio dimensijų priemonių įgyvendinimo organizacijoje būtinumą, bet ir identifikuoti galimas papildomas kibernetinio saugumo valdymo dimensijų priemones, kurios gali būti naudojamos, gerinant kibernetinio saugumo valdymo įgyvendinimą organizacijoje.

3.1. Kibernetinio saugumo valdymo modelio elektroniniams rinkimams įgyvendinti empirinio tyrimo rezultatų analizė

Atlikus siūlomo kibernetinio saugumo valdymo modelio empirinį tyrimą, buvo susisteminti ekspertinio tyrimo metu gauti rezultatai. Ekspertų atsakymai ir pastabos kibernetinio saugumo valdymo modeliui suteikė disertacijos autoriui galimybę patikslinti siūlomą kibernetinio saugumo valdymo modelį ir pateikti tam tikras modelio įgyvendinimo rekomendacijas organizacijoms, kurios, siekdamos efektyvaus

kibernetinio saugumo valdymo, nuspręs pasinaudoti šiuo kibernetinio saugumo valdymo modeliu savo organizacijos veiklos procesams modernizuoti.

Šiame poskyryje bus pateikiamos apibendrintos ekspertų nuomonės apie kibernetinio saugumo valdymo modelio tinkamumą kibernetinio saugumo valdymo srityje, taip pat pateikiami kibernetinio saugumo valdymo modelio empirinio tyrimo rezultatai.

3.1.1. Kibernetinio saugumo reiškinio konceptualizavimas

Siekiant konceptualizuoti kibernetinio saugumo sąvoką ir reiškinį (reiškinio suvokimą), tyrime dalyvavusių ekspertų pirmiausiai buvo klausiama apie kibernetinio saugumo reiškinio apibrėžimą ir buvo prašoma pateikti atsakymą, kaip kiekvienas ekspertas suvokia kibernetinį saugumą. Skirtingos tyrime dalyvavusių ekspertų nuomonės apie kibernetinio saugumo sąvoką ir reiškinį leidžia suprasti, dėl kokios priežasties kibernetinio saugumo terminas taip įvairiai traktuojamas ne tik mokslinėje literatūroje, bet ir informacinių technologijų atstovų gretose.

Kibernetinis saugumas ekspertų buvo apibrėžiamas labai įvairiais kontekstais:

1. *Technologinio saugumo užtikrinimo kontekstas*. Kibernetinis saugumas suvokiamas kaip „... techninės ir programinės įrangos tikslaus veikimo nustatymas ir užtikrinimas, siekiant apsaugoti informacinės sistemos veiklą ir joje esančių duomenų saugumą. Tik nuo informacinėje sistemoje esančios įrangos veikimo ir priklauso visos informacinės sistemos kibernetinis saugumas, o įrangos veiklos tęstinumas ir veiklos teisingumas gali būti užtikrintas kitais technologiniais sprendimais, pvz., veiklos sutrikimų stebėjimo sistemos, neįprasto kompiuterinio tinklo veikimo registravimo sistemos ir kt. Visiškas kibernetinis saugumas faktiškai nėra įmanomas, bet priartėti prie saugios informacinės sistemos realybės yra įmanoma tik panaudojant technologines sistemas.“ (4E, asmeninis interviu, 2019-09-23). Analogišką nuomonę išsakė ir 5E ekspertas, kuris pažymėjo, kad „... saugumas yra įmanomas tik tuomet, kai yra naudojama žinomų gamintojų, patikima ir technologiškai teisingai sukonfigūruota kompiuterinio tinklo įranga. Pastovus kompiuterinių sistemų, routerių, antivirusų ir kompiuterių programų atnaujinimas ir jų priežiūrą yra ne kas kita, kaip saugumą ir incidentų eliminavimą užtikrinantis faktorius.“ (5E, asmeninis interviu, 2019-09-27);
2. Kibernetinio saugumo suvokimas *technologinio, teisinio ir žmogiškojo faktoriaus įtakos* saugumui kontekste, kai „...yra naudojamos visos priemonės, kuriomis mes stengiamės apsaugoti visą savo įrangą, savo klientus (įstaigas, įmones), paslaugų vartotojus, visos technologinės, organizacinės ir teisinės priemonės, visų priemonių visuma. Visos priemonės, kurios užtikrina fizinį įrangos saugumą, informacijos saugumą (konfidencialumą, integralumą ir pasiekiamumą), kuris yra sudedamoji kibernetinio saugumo dalis. Kibernetinis saugumas yra ir žmonės, ir įranga, ir procesai bei jų teisinio reglamentavimo dalykai.“ (1E, asmeninis interviu, 2019-09-12). Panašią nuomonę apie kibernetinį saugumą išsakė ir 3E ekspertas, kuris pažymėjo, kad „...kibernetinis saugumas yra tik viena priemonė iš saugumo sampratos apskritai. Anksčiau saugumas reiškė gyvybę, o jo garantas

buvo karo kirvis. Nuosavybė – maistas, būstas, maisto ar kitos atsargos. Praradus ar kažkam pavogus karo kirvį, galėjai prarasti maistą, atsargas, taip pat ir santykinį saugumą, o kartais – ir gyvybę. Šios dienos realiame gyvenime praktiškai niekas nepakito, išskyrus tai, kad karo kirvio buvimo vieta nurodoma elektroninėje formoje, o duomenys apie tai saugomi kažkokiose elektroninėse laikmenose, kurias apdoroja tam sukurtos elektroninės sistemos. Kol laikaisi pagrindinių reikalavimų – konfidencialumo, vientisumo ir pasiekiamumo – tol gali jaustis sąlyginai saugus. Kibernetinis saugumas – tai žmonių suvokimo, techninių priemonių ir veiklos procedūrų laikymasis, saugant visus duomenis, kurie yra elektroninėje erdvėje.“ (3E, asmeninis interviu, 2019-09-17).

3. Kibernetinis saugumas suprantamas kaip *visapusiško kibernetinio saugumo* užtikrinimas, kai „.. atsiranda gebėjimas numatyti, išvengti ir suvaldyti grėsmes. Kai įmonė sugeba išvystyti tokį kibernetinį saugumą, kad gali ne tik tinkamai reaguoti į incidentus, bet ir išmokti juos numatyti. Išmokyti darbuotojus būti pasiruošusius atpažinti galimą grėsmę ir iš anksto imtis veiksmų. Būtent žmonių suvokimas, kad nesi saugus elektroninėje erdvėje, sudaro tam tikro kritinio mąstymo atsiradimą. Darbuotojų kritinis mąstymas ir mintis „*O kas, jeigu?*“ leidžia išvengti didelių problemų. Švietimas, komunikacija ir tinkamas požiūris į grėsmę suteikia pranašumo.“ (2E, asmeninis interviu, 2019-09-14). 6E ekspertas, apibūdindamas kibernetinį saugumą, sakė: „...puikiai tinka atnaujintas kibernetinio saugumo įstatymo kibernetinio saugumo apibrėžimas, kuris pasako, kad tai yra ne kas kita, kaip techninės, teisinės, informacijos sklaidos ir organizacinės priemonės, kuriomis siekiama išlaikyti atsparumą veiksniams, keliantiems grėsmę informacinėms sistemoms, jų veiklai ir jose esančiai informacijai. Šis apibrėžimas yra viską apimantis dalykas, kuris yra daug platesnis nei buvęs prieš tai ir orientuotas tik į kibernetinius incidentus. Dabar ir socialinės inžinerijos atakas ir bandymus formuoti netinkamą visuomenės nuomonę socialiniuose tinkluose galime drąsiai traktuoti kaip kibernetinio saugumo pažeidimą. Pagaliau sugebėjome išlipti iš paprasto technologinio požiūrio į kibernetinį saugumą ir supratome, kad IT nėra „*magic weapon*“ kibernetinėje erdvėje. Saugumas yra daugiau nei technologija“ (6E, asmeninis interviu, 2019-10-05). Atitinkamą nuomonę pateikė ir ekspertas 7E, kuris pažymėjo, kad „...Tai yra ne tik technologijos. Technologinių priemonių panaudojimas turi būti sumanus ir remtis prieš tai atlikta organizacijos veiklos procesų analize ir korekcija. Pirmiausia – visapusiškas mąstymas apie visas kylančias grėsmes, o tik paskui – priemonių šioms grėsmėms mažinti parinkimas. Ar tai technologija, ar rizikos valdymas, ar incidentų šalinimas, ar personalo švietimas, reikia noro keistis, vadovybės palaikymo, o tada jau galima galvoti, ką turi ir kaip pasikeisti. Nusipirkti programinę įrangą, parašyti taisykles, nusimatyti veiksmus krizės atveju, iškelti sau atitikties standartams reikalavimus ar dar kažkas. Pirmiausia suprask, kur tu nori keliauti ir turėk planą, o paskui ženk to tikslo link.“ (7E, asmeninis interviu, 2019-10-05). 8E ekspertas pažymėjo, kad „...sunku vienareikšmiškai duoti atsakymą į tą klausimą, kadangi bet kuri priemonė, kurios panaudojimas duos naudos ir padidins kibernetinį saugumą,

gali būti to kibernetinio saugumo sudedamoji dalis. Sumanus valdymas ir kibernetinių grėsmių suvokimas, tinkamų aptarnaujančių kompanijų ir jų siūlomų sprendimų parinkimas, žmogiškųjų išteklių kontrolė, teisinis reglamentavimas, ir visa kita. Visų tų dalykų panaudojimas apsisaugojimo nuo grėsmių kontekste ir yra kibernetinis saugumas. Nėra įmanoma užtikrinti šimtaprocentinio saugumo, bet tai nereiškia, kad visų galimybių išnaudojimas yra nereikalingas. Svarbu priartėti prie visiško kibernetinio saugumo per mažiausią atstumą ir žinoti, kad vis vien galima nukentėti, nei šaukti, kad visiško kibernetinio saugumo negalima užtikrinti ir nieko daugiau nedaryti, o visas bėdas „nurašyti“ užpuolikams. Tik tas, kas juda į priekį, gali save apsaugoti.“ (8E, asmeninis interviu, 2019-10-14). Panašios nuomonės apie kibernetinio saugumo reiškinį buvo ir 9E ekspertas, pažymėjęs, kad „... tai ne tik kompiuterinių sistemų apsauga, bet ir visos infrastruktūros ir išteklių apsauga, pasinaudojant visomis teisinėmis, techninėmis ir kitomis įmanomomis ir prieinamomis priemonėmis, siekiant sudaryti galimybę normaliai veikti ir išvengti bet kokių sutrikimų.“ (9E, asmeninis interviu, 2019-10-17).

Pažymėtina, kad daugumos kibernetinio saugumo valdymo modelio empiriniame tyrime dalyvavusių ekspertų pateikti atsakymai apie kibernetinio saugumo reiškinio apibrėžimą patį reiškinį apibūdina daug plačiau nei informacinių technologijų panaudojimą saugumo užtikrinimo kontekste. Ekspertai akcentuoja teisinius, socialinius, incidentų, rizikos, organizacijų valdymo ir kitus aspektus, kurie negali būti eliminuojami iš kibernetinio saugumo sąvokos. Tik visų įmanomų kibernetinio saugumo valdymo priemonių panaudojimas, gerinant organizacijos gebėjimą numatyti, prognozuoti ir, esant reikalui, kovoti su grėsmėmis, taip pat tinkamai vertinti šių priemonių panaudojimo efektyvumą, suteikia organizacijai galimybę vystyti savo atsparumą galimoms kibernetinėms grėsmėms, tokiu būdu gerinant kibernetinio saugumo valdymą.

Taip pat pažymėtina, kad ekspertai, pažymėję tik technologinio kibernetinio saugumo svarbą organizacijos kibernetinio saugumo užtikrinimo kontekste bei laikantys technologijas svarbiausia kibernetinio saugumo užtikrinimo priemone, pagal savo darbo pobūdį yra susiję su technologinio kibernetinio saugumo įgyvendinimu organizacijose. Atkreiptinas dėmėsis, kad empiriniame tyrime dalyvavę kibernetinio saugumo ekspertai, kurių darbas yra siejamas su organizacijos valdymo procesų kūrimu, organizacijos strateginių tikslų įgyvendinimu bei organizacijos veiklos pokyčių kibernetinio saugumo aspektais koregavimu, buvo linkę vertinti kibernetinį saugumą ir jo valdymą daug platesniame kontekste, kuris apima ne tik technologinius procesus, bet ir visus kitus (socialinius, teisinius, procedūrinius ir kt.) kibernetinio saugumo valdymo aspektus.

Vadovaujantis kibernetinio saugumo ekspertų pareikštomis nuomonėmis, taip pat pasaulio mokslininkų ir kibernetinio saugumo ekspertų pateiktais kibernetinio saugumo apibrėžimais, darytina išvada, kad kibernetinis saugumas šiuolaikiniame pasaulyje, kuris yra neįsivaizduojamas be informacinių ir ryšių technologijų, turi būti traktuojamas ne tik kaip technologinė disciplina, bet labiau kaip reiškinys, kuris sujungia savyje technologines, socialines, vadybos ir kitas mokslo šakas, o to sujungimo tikslas yra suteikti piliečiams, organizacijoms ir jų nariams žinių, galinčių padėti apsisaugoti nuo grėsmių ir pažeidžiamumų, egzistuojančių šiame skaitmenizuotame pasaulyje.

3.1.2. Organizacijos valdymo procesų įtaka kibernetiniam saugumui

Nagrinėjant kibernetinio saugumo valdymo modelio organizacijos valdymo procesų dimensiją, tyrime dalyvavę ekspertai pateikė vieningą nuomonę apie šios dimensijos svarbą ir įtaką kibernetinio saugumo valdymui organizacijoje. Visi ekspertai pareiškė, kad organizacijos valdymo procesų įtaka kibernetinio saugumo užtikrinimo procese yra svarbi, tačiau šis palaikymas ekspertų yra suprantamas šiek tiek skirtingais aspektais, kai:

1. *Kibernetinis saugumas* suprantamas kaip *neatsiejama organizacijos valdymo procesų sudedamoji dalis.* Atsakydamas į pateiktus klausimus, 1E ekspertas pažymėjo, kad „... tai yra sudedamoji dalis kibernetinio saugumo, ir procesus reikia adaptuoti taip, kad būtų įvertintas kibernetinis saugumas. Kibernetinis saugumas ir jo suvokimas, nežinau, kokiu aspektu padeda valdyti, ekonominiu, saugumo ar kitokiu, bet jis padeda organizacijos brandai apskritai. Didina organizacijos brandą ir kartu sumažina rizikas, tačiau tai priklauso ir nuo pačios organizacijos dydžio ir to saugumo poreikio. Jei riši ir parduodi vantas, tai klausimas, ar tau reikia kibernetinio saugumo. Bet orientuokimės ne į smulkųjį verslą, organizacija organizacijai nelygi. Kiekviename projekte kibernetinis saugumas turi būti vertinamas ir tik nuo to projekto svarbos organizacijai priklauso kibernetinio saugumo dedamosios įtraukimas į organizacijos valdymo procesus. Kiekvienoje organizacijoje privalo būti kažkas, kas yra atsakingas už kibernetinį saugumą. Tas žmogus ar padalinys turi būtinai turėti organizacijos vadovo palaikymą. Palaikymas yra privalomas, o atsakingi gali būti ir CERT komanda, ir saugumo pareigūnas ar net IT departamentas. Būtinas toks padalinys ir jo palaikymas iš vadovų, nes kitaip atsiranda didelis kitų narių pasipriešinimas, nes sauga dažniausiai trukdo darbui.“ (1E, asmeninis interviu, 2019-09-12). Tyrimo metu 2E ekspertas pateikė analogišką nuomonę, pažymėdamas, kad „... būtent nuo kibernetinio saugumo supratimo organizacijoje, pirmiausia vadovo lygmenyje, toliau tarp jos padalinių ir organizacijos narių ir priklauso šio proceso sėkmė. Jei vadovas nesupranta, kad mums, jam reikia apsaugoti savo resursus, duomenis, reputaciją, tai jis negali būti vadovu. Nesuderinami dalykai. Pats kibernetinis saugumas modernioje organizacijoje turi būti ne *„ad hoc“* darbu, o kasdieniu procesu, kuris privalo būti atliekamas kiekvieną dieną, o kiekvienas projektas turi prasidėti, iškarto vertinant kibernetinio saugumo aspektą, kad ateityje nebūtų skaudu ir finansiškai brangu. O jei jau atsirado supratimas apie kibernetinių grėsmių egzistavimą ir mes pradedam tinkamai vertinti kibernetinio saugumo būtinumą, tai reiškia tik viena – subrendom. Tuomet reikia pažiūrėti, kokia situacija yra dabar, apsibrėžti, ką mes norim pasiekti. Pažiūrėti, įvertinti ir pagalvoti, kokiais būdais ir priemonėmis mes galime keistis. Ką turim padaryti, kad tobulėtume, kad pokyčiai padėtų pasiekti reikalingą tikslą.“ (2E, asmeninis interviu, 2019-09-14). Panašios nuomonės, atsakydamas į pateiktus klausimus, buvo ir 3E ekspertas, kuris pažymėjo, kad kibernetinio saugumo valdymo įtaka organizacijai yra „... tiesioginė, tačiau ir santykinė. Didžioji dalis organizacijų nesivargina

vertinti rizikas, kurios per kibernetinį saugumą gali turėti įtakos organizacijos valdymui, tačiau kibernetinio saugumo valdymo reiškinio supratimas ir naudojimas organizacijoje, jos valdymo sistemoje bei tarp organizacijos narių tiesiogiai daro įtaką pačios organizacijos kibernetinio saugumo užtikrinimo procesui. Įsivaizduokite, kad kibernetinis saugumas – tai automobilis ar apšvietimas biure ar pan. Ar tai yra kasdieniai neatsiejami dalykai, be kurių organizacijos veikla būtų iš dalies ar visiškai paralyžiuota? Taip. O saugumo reikšmė organizacijos projektuose? Atsakysiu klausimu: kokią reikšmę organizacijos vykdomuose projektuose turi finansiniai aspektai? Tik blogas finansavimo plano vykdymas viename organizacijos projekte dažnai neigiamai veikia ne visos organizacijos gyvybingumą, o vienas kibernetinis incidentas gali būti ir paskutinis šiai organizacijai. Šiame kontekste ir slypi esmė. Kibernetinis saugumas yra labai svarbus ir pagal jo reikalavimus reikia tvarkytis, koreguoti savo veiklą, vidinius procesus." (3E, asmeninis interviu, 2019-09-17). 6E ekspertas, atsakydamas į klausimus, pažymėjo, kad „... kibernetinis saugumas veikia organizaciją tiesiogiai, bet, atsižvelgiant į organizacijos dydį ir struktūrą bei į sprendimus priimančių žmonių suvokimą / išprusimą apie kibernetinį saugumą, saugumo supratimas lemia tikimybę patirti finansinę, ir ne tik, žalą organizacijai bei žmogiškiesiems ištekliams. Organizacijoje turi būti nuolat (nustatytais periodais, pvz., kas ketvirtį) vykdomas personalo mokymas, supažindinimas su naujomis, esamomis kibernetinio saugumo grėsmėmis, pasekmėmis ir prevencinėmis priemonėmis. Kibernetinio saugumo dedamoji reikšmė organizacijos vykdomuose (naujai įgyvendinamuose) projektuose yra viena iš dedamųjų, tačiau nepastovi / kintama, atsižvelgiant į atliktos rizikos analizę bei organizacijai priimtiną rizikos laipsnį, tačiau, siekiant geresnio atsparumo kibernetinėms grėsmėms, nustatytu periodiškumu būtų tikslinga peržiūrėti ir, esant poreikiui, atlikti organizacijos valdymo procesų peržiūrą ir koregavimą." (6E, asmeninis interviu, 2019-10-05). 7E ekspertas, atsakydamas į klausimą, pasakė: „... būtent vadovas ir turi pateikti viziją, kokia turi būti saugi organizacija. Tik turint aiškią organizacijos ateities viziją, gali kurti savo tikslo pasiekimo strategiją. Supratęs, kur tu nori būti po vienerių, trejų, penkerių metų, ir atlikęs analizę, suprasi, ko tau reikia, norint pasiekti tikslą. Visų pirma, reikia suprasti, kad nėra visiško saugumo, o kibernetinio saugumo užtikrinimas įmanomas tik tuomet, kai visi prisideda prie jo kūrimo. Geriausias dalykas, kai vadovas suvokia, kad tik nuo jo priklauso, kaip bus organizuojamas ir kuriamas organizacijos kibernetinio saugumo valdymas. Kai vadovas supranta, kad reikia keistis ir nelaukti, kol koks nors incidentas sužlugdys organizacijos darbą. Organizacija privalo keistis, o pokyčio pradžios mechanizmo paleidimo mygtukas yra vadovo rankose. Taigi, nuspaudei ir procesas prasideda. Pradės keistis vadovų supratimas, pasikeis ir pavaldinių, nes kitaip turbūt bus ne pakeliui." (7E, asmeninis interviu, 2019-10-05). 9E ekspertas pažymėjo, kad „... kibernetinis saugumas organizacijoje turi būti suprantamas kaip produktas (elementas), kuris turėtų sąveikauti su visais procesais. Jis būtinas organizacijos valdyme. Taip atsiranda suvokimas, kad kibernetinio saugumo integravimas į visus be išimties

organizacijos veiklos procesus yra reikalingas, tokiu būdu nustatant privalomų korekcijų būtinybę.“ (9E, asmeninis interviu, 2019-10-17). 8E eksperto nuomonė buvo analogiška anksčiau išsakytoms nuomonėms, tačiau, pažymėdamas kibernetinio saugumo reiškinio svarbą, jis pabrėžė vieną esminį aspektą: „... sumanus valdymas yra labai gerai. Modernių dalykų įtaka vadovams taip pat yra gera, tačiau kas įtikins organizacijos direktorių, kad mes irgi esame pažeidžiami. Kol kažkas nenutinka, tol visi nekreipia dėmesio, o kai nutinka, jau būna vėlu. Visi kalba, kad saugumas yra neatsiejama valdymo, veiklos procesų dalis, tačiau kaip įtikinti vadovą, kad mes esame pažeidžiami? Labai sunku būdavo anksčiau, dabar šiek tiek paprasčiau, nes, kai nuskamba, kad kažkas nesirūpino saugumu ir patyrė finansinių nuostolių ne vien dėl kompiuterio gedimo, o dėl duomenų užšifravimo, kai sužinomos nuostolių sumos, teoremos įrodinėjimas supaprastėja.“ (8E, asmeninis interviu, 2019-10-14);

2. Kibernetinio saugumo *grėsmės* per organizacijos valdymo procesus ir finansavimą *daro įtaką technologinio kibernetinio saugumo užtikrinimui.* Technologinio kibernetinio saugumo užtikrinimo svarbą pažymėjo 4E ekspertas, atsakydamas į pateiktus klausimus: „... organizacijos valdymas vienareikšmiškai veikia kibernetinį saugumą. Pagalvokime apie įrangai skiriamas lėšas. Svarbu, kad vadovas ir kolegos suprastų, kad yra grėsmės. Tuomet galima aptarti grėsmes ir nuspręsti, kaip jų išvengti. Surasime tinkamą įrangą ir eliminuosime galimas grėsmes, o vykdydami kažkokį projektą, iškart žiūrėsime, kaip kibernetinis saugumas darys įtaką pinigams. Vis tik, vertinant kibernetinį saugumą, reikia turėti palaikymą iš vadovybės, kitaip, suprastėjus finansavimui, negalėsime užtikrinti sistemų veiklos ir sistemose esančių duomenų saugumo.“ (4E, asmeninis interviu, 2019-09-23). 5E ekspertas tai pat pateikė panašią nuomonę, pažymėdamas, kad „... vadovybės supratimas yra labai svarbus ir tik nuo vadovo priklauso finansavimas. Dabartiniu momentu labai daug grėsmių, privalai jas visas nusimatyti ir išspręsti, kokiais produktais jas pašalinsi, nes negali visko uždrausti darbuotojams be papildomos techninės ar programinės įrangos. O vadovybės palaikymas ir apsaugai skiriamas tinkamas finansavimas palengvina kibernetinio saugumo užtikrinimo procesą.“ (5E, asmeninis interviu, 2019-09-27).

Pažymėtina, visi kibernetinio saugumo ekspertai, vertindami organizacijos valdymo procesų įtaką kibernetiniam saugumui, vienareikšmiškai teigia, kad kibernetinio saugumo valdymas yra tiesiogiai priklausomas nuo organizacijos vadovybės supratimo ir palaikymo. Kiekviena organizacija vienareikšmiškai turi suvokti, kad šiuolaikiniame pasaulyje egzistuoja aibė grėsmių, kurių panaudojimas prieš organizaciją gali sukelti neigiamų padarinių. Tik visos organizacijos supratimas apie jai gresiančius pavojus ir noras keistis bei aiškaus pokyčių plano identifikavimas suteikia organizacijai galimybes atlikti reformas, kurios priartins organizaciją prie kibernetinio saugumo užtikrinimo. Tyrimo metu ekspertų pateikti atsakymai patvirtina pasaulio mokslininkų išreikštas nuomones, kad organizacijos savo veiklos procesus privalo analizuoti ir organizuoti kompleksiškai, atsižvelgiant į dabartiniais laikais egzistuojančias kibernetines grėsmes (Deighton, 2015; Latham & Watkins, 2016; Limba ir kt., 2017; Moschovitis, 2018).

Tyrime dalyvavę ekspertai taip pat buvo klausiami apie priemones, kurias organizacija turi naudoti, siekdama pagerinti organizacijos valdymo procesus. Apibendrinant ekspertų pateiktus atsakymus, galima teigti, kad, siekdama organizacijos valdymo procesų dimensijos pokyčių, organizacija turi imtis toliau išvardytų priemonių: nusistatyti tikslus, identifikuoti pokyčio proceso dalyvius, valdymo sistemą ir sprendimų priėmimo procesą bei veiklos standartus; parengti pokyčių planą, nusistatyti būtinas organizacijos narių kompetencijas, identifikuoti atsakomybės ribas ir organizacijos aplinką bei nusimatyti pokyčiams būtinus resursus ir pajėgumus.

Būtina pažymėti, kad empiriniame tyrime dalyvavusių kibernetinio saugumo ekspertų nuomonės ir interviu metu gauti paaiškinimai dėl tam tikrų identifikuotų kibernetinio saugumo gerinimo priemonių įgyvendinimo, siekiant patobulinti kibernetinio saugumo valdymą organizacijoje, bus panaudoti, tikslinant disertacinio darbo autoriaus sukurtą kibernetinio saugumo valdymo modelį.

3.1.3. Teisinio reguliavimo įtaka kibernetiniam saugumui

Nagrinėjant kibernetinio saugumo valdymo modelio teisinio reguliavimo dimensiją ir siekiant nustatyti jos įtaka kibernetinio saugumo valdymui, ekspertams empirinio tyrimo metu buvo pateikti klausimai, kurie padėtų išgryninti bendrą požiūrį į teisinio reguliavimo aspektų svarbą bei jų įtaką kibernetinio saugumo valdymui organizacijos kontekste.

Visi empiriniame tyrime dalyvavę ekspertai, pareikšdami savo nuomonę apie teisinio reguliavimo aspektų įtaką kibernetinio saugumo valdymui, pateikė atsakymus, kurie leidžia vienareikšmiškai teigti, kad teisinis reguliavimas yra neatsiejama kibernetinio saugumo valdymo dedamoji, tačiau pats teisinis reguliavimas kibernetinio saugumo valdymo kontekste bei išorės ir vidaus aplinkų poveikis teisiniam reguliavimui organizacijoje yra suprantami skirtingai, o ekspertų pateiktas nuomones galima suskirstyti į dvi grupes, kuomet:

1. Teisinis reguliavimas yra suprantamas kaip organizacijos *personalo veiklos reglamentavimas kibernetinio saugumo kontekste,* sudarantis organizacijai galimybes nusistatyti jos narių veiklai taikomus apribojimus. 6E ekspertas, atsakydamas į pateiktus klausimus, pareiškė nuomonę, kad „... tai yra ne kas kita, kaip atsakomybės priskyrimas žmogiškiesiems ištekliams, priklausomai nuo jiems suteiktų prieigų ir atsakomybių kibernetinio saugumo srityje. Ar tai būtų vartotojas, administratorius ar informacinės sistemos valdytojas, kiekvienas turi turėti veiklos instrukcijas ir daryti tik tai, ką jam yra leidusi organizacija. Būtent organizacija turi nuspręsti, kaip turi būti reguliuojama darbuotojų veikla kibernetinėje erdvėje, o darbuotojas privalo šiam reguliavimui paklusti. O kalbant apie organizacijos aplinkų svarbą kibernetinio saugumo prasme, galiu pasakyti tik tiek, kad vidaus aplinkos poveikis teisiniam reguliavimui yra daug svarbesnis, nes kiekviena organizacija pati sprendžia, kas yra leistina, o kas draudžiama, ir jau pagal tai sprendžia, kokius įsakymus parengti ir kaip reglamentuoti darbą. Atsižvelgiant į organizacijos dydį, vykdomą veiklą, finansinius išteklius bei resursus, teisinis reguliavimas balansuotų tarp privalomos ir rekomenduotinos ribos. Priklausomai

ar prevencinės priemonės bus įformintos tik „popieriuje“, ar bus bandoma teisinė reguliavimą modeliuoti numatomam ar prognozuojamam kibernetiniam incidentui.“ (6E, asmeninis interviu, 2019-10-05). Panašią nuomonę pateikė ir 3E ekspertas, atsakydamas, kad „... teisinis reguliavimas turi būti realizuotas per organizacijos teisėkūros kontekstą. Bet kokie teisinio reguliavimo procesai privalo būti suderinti su organizacijos kibernetinio saugumo reglamentavimu. Kitaip sakant, organizacija nusistato, kas yra leistina ir saugu daryti jos valdomoje infrastruktūroje, parengia tvarkas ir nurodymus bei su šiais nurodymais supažindina savo personalą, kuris turi jos vykdyti. Tačiau nepamirškime ir privalomų teisinių reikalavimų iš išorės. Negalima sudaryti darbuotojui tokių sąlygų, kad jis būtų nuolat sekamas ir nieko negalėtų padaryti be organizacijos žinios. Jei stebime ir ribojame visus jo veiksmus, tai ar mes neprasilenksime su asmens duomenų apsaugos reikalavimais, darbuotojo teise į privatumą? Pasirenkant savo veiksmus, būtina galvoti, kad jie nebūtų pertekliniai, o darbuotojas nesijaustų nuolat sekamas.“ (3E, asmeninis interviu, 2019-09-17). Analogiškos nuomonės laikėsi ir 4E ekspertas, kuris teisinį reguliavimą identifikavo kaip „... darbo instrukcijų ir elgesio taisyklių rinkinius. Organizacija parengia vidinius įsakymus, tvarkas ir taisykles, kurios numato griežtą darbuotojų veiklos reglamentavimą. Įsidarbinai, susipažinai ir veiki pagal instrukcijas, o jei nori kažką veikti Facebook'e ar kaip administratorius eksperimentuoti, tai tą gali padaryti savo telefone arba bandomojoje sistemoje. Žaidimo taisykles nustato darbdavys, kurio resursus tu neturėtum naudoti savo reikmėms ar eksperimentams, nes tai yra jo turtas, kuris jam tarnauja kaip darbo įrankis, o jo gedimas atneša nuostolių bei didina įmonių išlaidas.“ (4E, asmeninis interviu, 2019-09-23).

2. Teisinio reguliavimo įtaka kibernetiniam saugumui yra suprantama kaip *išorinės aplinkos poveikis organizacijai, skatinantis ją įgyvendinti vidinius* teisinio *reguliavimo mechanizmus.* 1E ekspertas, atsakydamas į klausimus, pareiškė nuomonę, kad „... teisinis reguliavimas yra būtinas, bet ne tik tam, kad darbuotojai žinotų taikomus apribojimus ir ribas, bet žinotų ir tai, kokia yra kibernetinį saugumą užtikrinančio personalo rolė organizacijos veikloje, ką tas personalas gali daryti. Ir tie, kas dirba organizacijoje, ir tie, kas ją saugo nuo tam tikrų kibernetinių pavojų, privalo veikti pagal instrukcijas ir pagal nustatytas žaidimo taisykles. O tos taisyklės atsiranda ne tik nuo organizacijos norų, bet ir nuo išorinės aplinkos poveikio, teisės aktų reikalavimų ir kitokių dalykų. Tas, kas yra viduje, yra svarbu, bet išorinė aplinka yra daug svarbesnė. Tai, kas yra viduje, negali viršyti išorinių reikalavimų, pavyzdžiui, duomenų apsaugos reglamento reikalavimų ir t. t. Vidinis reguliavimas turi bent jau neprieštarauti išoriniam, o jei kalbam apie valstybės valdymo organizacijas ar valstybės informacinių sistemų valdytojus, tai jiems išorinis reguliavimas yra daug svarbesnis, kadangi būtent tas išorės poveikis ir sudaro būtinumą vidiniam reguliavimui, jo tobulinimui ir pastoviam stebėjimui.“ (1E, asmeninis interviu, 2019-09-12). Analogiškos nuomonės laikėsi ir 2E ekspertas, kuris pažymėjo, kad „... negalime kalbėti tik iš vidinių pokyčių pozicijos. Žinoma, visos tos vidaus tvarkos taisyklės yra būtinos, bet pažiūrėkime,

iš kur atsiranda jų poreikis? Gal tai ne būtinai kažkokių teisės aktų poveikis organizacijai. Pavyzdžiui, verslas ne visada vadovaujasi teisės aktais, kurdamas savo IT skyrius, duomenų apsaugos pareigūnus ar dar kažkokias kibernetinio saugumo pozicijas. Verslui svarbu susimažinti išlaidas, bet ir atitikti tam tikrus standartus tuo pat metu. Tai traktuokime tuos standartus kaip teisinio reguliavimo analogą privačiame sektoriuje. Jis veikia organizaciją ir ji keičiasi. Išorinės aplinkos poveikis yra svarbesnis už vidinės, net sakyčiau, jis sąlygoja vidinės aplinkos pokyčius." (2E, asmeninis interviu, 2019-09-14). 5E ekspertas pažymėjo, kad „...teisinis reguliavimas labai svarbus, bet jis neapsiriboja tik vidinėmis tvarkomis ir draudimais. Daug svarbiau yra tai, dėl ko atsiranda tas reguliavimas, ir ar tu, būdamas organizacijos vietoje, gali jai daryti įtaką. Gali viduje daryti viską, kas neprieštarauja teisinei bazei, bet vargu ar paveiksi išorę. Greičiausiai, jei tu esi privati bendrovė, tai tu jokios įtakos išorės teisiniam reguliavimui nepadarysi, bet, jei tu esi viešojo sektoriaus atstovas, tai tu gal ir galėtum daryti įtaką teisinio reguliavimo normoms. Gal ne tiek daryti įtaką, o labiau reikalauti jas tikslinti, jei yra kažkokių nesusipratimų šioje srityje. Vidaus teisinis reguliavimas labai svarbus, bet svarbiau yra išorinė aplinka, kuri dažniausiai sąlygoja vidinių taisyklių pakeitimus." (5E, asmeninis interviu, 2019-09-27). Analogiškus argumentus išsakė 7E, 8E bei 9E ekspertai, pažymėdami, kad organizacijos teisinio reguliavimo sistema daugumoje atvejų priklauso nuo ją supančios aplinkos: „viešojo sektoriaus atstovams yra sukuriami teisinio poveikio mechanizmai ir reikalavimai" (9E, asmeninis interviu, 2019-10-17), o privatus sektorius, įvesdamas teisinį kibernetinio saugumo reguliavimą, dažniausiai vadovaujasi „gerosiomis praktikomis" (7E, asmeninis interviu, 2019-10-05) bei „atitikties standartais" (8E, asmeninis interviu, 2019-10-14), tačiau „taisyklės yra būtinos visiems ir visi privalo jų laikytis" (9E, asmeninis interviu, 2019-10-17).

Apibendrinant ekspertų pateiktas nuomones, galima teigti, kad dauguma empiriniame tyrime dalyvavusių kibernetinio saugumo ekspertų mano, kad teisinio reglamentavimo dimensija yra labai svarbi kibernetinio saugumo valdymui įgyvendinti. Pasak ekspertų, būtent šios dimensijos įgyvendinimas pakloja pamatus saugiam darbuotojų elgesiui kibernetinėje erdvėje, naudojantis organizacijos turimais ištekliais, bei reglamentuoja darbuotojų elgesio taisykles. Ekspertai patvirtino šios dimensijos svarbą, kuri taip pat yra aptariama pasaulio mokslininkų darbuose (Štitilis, 2013; Appazov, 2014; Deighton, 2015; Latham & Watkins, 2016; Brisch, 2017; Limba ir kt., 2017; Kosseff, 2018). Taip pat būtina pažymėti, kad dauguma tyrime dalyvavusių ekspertų išorinės aplinkos poveikį organizacijos kibernetinio saugumo valdymo modelio teisinio reguliavimo dimensijai įvardina kaip daug svarbesnį nei vidinės aplinkos poveikį.

Empirinio tyrimo metu ekspertams taip pat buvo užduotas klausimas apie tai, kokių priemonių privalo imtis organizacija ir kokie veiksmai turi būti atlikti, siekiant tobulinti organizacijos teisinio reguliavimo aspektus kibernetinio saugumo valdymo kontekste. Apibendrinant ekspertų pateiktas nuomones, galima teigti, kad, norint tinkamai organizuoti teisinio reguliavimo dimensijos įgyvendinimą, būtina imtis šių priemonių: išanalizuoti organizacijos teisinio reglamentavimo sistemą ir nustatyti jos

trūkumus; identifikuoti organizacijos veiklos tęstinumui reikalingus pokyčius; parengti ir patvirtinti teisinio reglamentavimo dokumentus, reikalingus organizacijos veiklos tęstinumui užtikrinti; vykdyti teisės aktų ir taisyklių taikymo bei naudojimo organizacijoje vertinimą. Tyrimo metu ekspertų pateikti atsakymai ir nuomonės apie tam tikrų kibernetinio saugumo teisinio reguliavimo priemonių panaudojimą, gerinant šią kibernetinio saugumo valdymo modelio dimensiją, bus panaudoti, tikslinant šio disertacinio darbo autoriaus sukurtą kibernetinio saugumo valdymo modelį.

3.1.4. Kibernetinio saugumo kultūros įtaka kibernetiniam saugumui

Nagrinėjant organizacijos kibernetinio saugumo kultūros įtaką kibernetinio saugumo valdymui organizacijoje, empirinio tyrimo dalyviams buvo pateikti klausimai, susiję su kibernetinio saugumo kultūros kūrimo organizacijoje aspektais, apimančiais personalo valdymo, mokymo ir kitus su žmogiškųjų išteklių valdymu susijusius klausimus. Kuriant kibernetinio saugumo valdymo modelį, kibernetinio saugumo kultūros dimensijos kūrimas labiausiai buvo siejamas su žmogiškojo faktoriaus įtaka kibernetinio saugumo valdymo reiškiniui.

Ekspertai, atsakinėdami į empirinio tyrimo metu pateiktus klausimus, vienareikšmiškai pripažino kibernetinio saugumo kultūros aspekto svarbą, užtikrinant kibernetinio saugumo valdymą, taip pat pateikė atsakymus ir paaiškinimus, kurie patikslino disertacinio darbo autoriaus siūlomo kibernetinio saugumo valdymo modelio kibernetinio saugumo kultūros dimensijos įgyvendinimo priemones, padėsiančias organizacijai gerinti saugumo situaciją.

Įvardinant kibernetinio saugumo kultūros dimensijos įgyvendinimo problematiką organizacijoje, ekspertų nuomonė apie probleminių aspektų egzistavimą buvo vieninga, tačiau nuomonės apie problemų atsiradimo priežastis gali būti suskirstytos į keturias grupes, kai:

1. Kibernetinio *saugumo svarba nesuvokiama* organizacijos *informacinių technologijų naudotojų gretose* sudaro galimybes kibernetinio saugumo incidentams ir nuostoliams atsirasti. E1 ekspertas, įvardindamas kibernetinio saugumo kultūros organizacijoje problemas, pateikė nuomonę, kad „... didžiausia problema yra tos kultūros nebuvimas. Būtent tos kultūros nebuvimas ir lemia problemas kibernetinės saugos srity. Žmogiškasis faktorius yra lemiama dedamoji šiuo atveju. Organizacijos branda, jos pažangumas, net elementari kibernetinė higiena lemia organizacijos kibernetinės kultūros buvimą. Kuo labiau darbuotojai supranta kibernetinio saugumo svarbą, tuo lengviau jį valdyti organizacijoje, tuo lengviau dirbti organizacijos CERT komandai. Žmonės yra pagrindinė problema. Tie, kurie naudoja technologijas kasdieniam darbui, dažniausiai dėl savo nežinojimo sukelia kibernetinius incidentus.“ (1E, asmeninis interviu, 2019-09-12). 4E ekspertas, pateikdamas savo nuomonę apie problematiką, pažymėjo, kad „...didžiausia problema yra žmogus. Darbuotojo ar sistemos naudotojo nesuvokimas, kad saugumo mechanizmai yra naudojami ne tam, kad apribotų jo galimybes užsiimti pašaliniais darbais darbo metu, o tam, kad apsaugotų įmonės turtą nuo pažeidžiamumų, yra tiesiog nesuprantamas. Darbuotojas tiesiog

nesuvokia, kad elementarus apsisaugojimas nuo kibernetinių grėsmių yra būtinas, o neadekvatūs veiksmai elektroninėje erdvėje gali padaryti labai daug nepataisomos žalos. Trūksta suvokimo apie elementarius dalykus, nesupratimas ir „kibernetinės higienos“ nesuvokimas yra didžiausia problema.“ (4E, asmeninis interviu, 2019-09-23);

2. Kibernetinio *saugumo svarba nesuprantama arba netaikoma organizacijos vadovams.* Tokia situacija suponuoja kibernetinio saugumo specialistų pastangų nesupratimą vadovaujančiame lygmenyje, o tai automatiškai sukelia trikdžius, susijusius su kibernetinio saugumo kultūros dimensijos priemonių įgyvendinimu organizacijoje. 6E ekspertas pažymėjo, kad „...pagrindinė problema yra vadovaujančio personalo, sprendimo priėmėjų nesuvokimas, kad kibernetinis saugumas yra svarbus. Jie galvoja, kad pasisamdo darbuotojus su žiniomis, kurių visiškai pakanka tam, kad būtų užtikrintas kibernetinis saugumas organizacijoje. Bet dažniausiai yra pamirštama apie tai, kad reikalingas mokymas, būtinas supažindinimas su esamomis problemomis bei priminimas išmoktų pamokų, prognozuojamų incidentų nagrinėjimas, iššūkių kibernetinėje saugumo aplinkoje tyrinėjimas. Tiesiog galvojama, kad viso to nereikia, nes tai nieko gero nepadaro, o tiems dalykams skirti pinigai verčiau turi būti panaudoti technologinei įrangai pirkti.“ (6E, asmeninis interviu, 2019-10-05). Šiek tiek kitokią poziciją pateikė 3E ekspertas, kuris pažymėjo, kad „...pagrindinė kibernetinio saugumo kultūros problema organizacijoje yra organizacijos vadovų nesuvokimas ir nesusivokimas saugumo klausimais. Priešingu atveju apie problemą nekalbėtume. Problemos sprendimo būdas tik vienas – vadovų mokymai, pradedant bendravimo su aplinkiniais kultūra ir baigiant kibernetiniu saugumu. Dažnai vadovas negalvoja, kad kibernetinis saugumas yra grėsmė ir jos reikia visais įmanomais būdais vengti. Jei vadovas ir supranta, tai žino, kad reikia apriboti darbuotojų teises, o jis pats turi „prigimtinę vadovo“ teisę daryti ką nori: siųstis torentus, naršyti internete be antiviruso. Keistas požiūris. Toks jausmas, kad žmogus nesuvokia, kad grėsmės nesirenka asmenų pagal pareigas, jos visiems yra vienodos.“ (3E, asmeninis interviu, 2019-09-17);
3. Kibernetinio *saugumo reikalavimų nesupranta ir nesilaiko informacinių technologijų sistemas* ir duomenų perdavimo tinklus *aptarnaujantis personalas.* Toks technologines ir programines įrangas aptarnaujančio personalo elgesys sudaro padidintas rizikas kibernetinio saugumo incidentams atsirasti. 2E ekspertas pažymėjo, kad „... didelė problema yra kompiuterių administratorių pasitikėjimas savimi. Kodėl jie galvoja, kad yra nepažeidžiami? Jie gal ir daug žino apie atakas, bet tai nesuteikia jiems labai didelio pranašumo. Atakas planuoja žmogus, o dažniausiai jis veikia ne vienas ir tikrai nėra naivus, o kartais atakas orientuoja būtent į administratorius, nes žino, kad jie kartais per daug pasitiki savimi. Kam reikia dirbti administratoriaus teisėmis, kai tu neadministruoji kompiuterių. Koks tikslas? Patogumas? Gal reikia kartais pabūti paranoišku ir galvoti, kad pats gali tapti atakos taikiniu.“ (2E, asmeninis interviu, 2019-09-14). Panašios nuomonės apie kibernetinio saugumo kultūros problemą buvo ir 7E ekspertas, atsa-

kydamas, kad „...mane labai stebina labai gera sistemų administratorių nuomonė apie save. Jiems nieko negali nutikti. Dirba ignoruodami kibernetinio saugumo specialistų ir saugumo pareigūnų rekomendacijas. Labai dažnai net nebando tobulintis ir viską daro taip, kaip yra įpratę, nors grėsmių pobūdis jau seniai pasikeitė. Taisyklių nepaisymas, nenoras tobulėti ir darbas iš įpročio dažniausiai ir lemia problemų atsiradimą. Manau, kad administratorius turi būti pavyzdys visiems kitiems, o viena iš pagrindinių funkcijų yra ne tik valdyti sistemas, bet ir dalyvauti naudotojų edukacijos procese.“ (7E, asmeninis interviu, 2019-10-05);

4. Kibernetinio *saugumo problemų atsiradimą lemia visos organizacijos narių* kibernetinio saugumo įgūdžių stoka. Visų tyrime dalyvavusių kibernetinio saugumo ekspertų išsakytų nuomonių sintezę, pasak kibernetinio saugumo ekspertų 5E, 8E ir 9E, lemia kibernetinio saugumo kultūros stoka organizacijoje. Ekspertai pažymėjo, kad „... neįmanoma pasakyti, kuris iš organizacijos narių gali būti atsakingas už kibernetinio saugumo problemos atsiradimą. Vienareikšmiškai negali pasakyti, kad kaltas yra vienas ar kitas. Kiekvienam reikia pradėti nuo savęs. Tik tuomet, kai pasitobulinsi saugos plotuose, galėsi pasakyti, kad aš tikrai nesu silpnoji grandis.“ (8E, asmeninis interviu, 2019-10-14), kad „... vien tik toks integruotas bei visus organizacijos narius vienijantis požiūris į kibernetinio saugumo problemą gali užtikrinti jos mąsto sumažėjimą arba bent jau logišką kontrolę.“ (5E, asmeninis interviu, 2019-09-27). Atkreiptinas dėmesys, kad „... organizacijos investuoja milžiniškus išteklius į technologijos palaikymą, tačiau mažai investuoja į visų savo darbuotojų kibernetinio saugumo įgūdžių tobulinimą, švietimą. Veiksmingiausias būdas apsisaugoti – investuoti į žmogiškąjį elementą, sukurti brandžią saugumo suvokimo tobulinimo programą, kuri galės pakeisti personalo elgesį, taip sudarydama galimybę kibernetinio saugumo kultūros ir tradicijų atsiradimui organizacijoje.“ (9E, asmeninis interviu, 2019-10-17).

Nagrinėjant organizacijos poziciją partnerystės ar paslaugų iš kitų organizacijų teikimo klausimais, ekspertai buvo apklausiami apie galimybes ir būtinumą reikalauti, kad kitos organizacijos, kurios pagal savo veiklos pobūdį bendradarbiauja ar teikia jai paslaugas, įgyvendintų kibernetinio saugumo kultūros priemones. Ekspertai pateikė atsakymus, kurie gali būti suskirstyti į trys grupes, kai manoma, kad:

1. Organizacijai yra *privaloma bendradarbiauti tik su patikimais* partneriais, kadangi partnerių kibernetinis saugumas gali neigiamai veikti organizacijai kylančias kibernetinio saugumo grėsmes. Atsakydamas į pateiktą klausimą, 1E ekspertas pažymėjo, kad „... tai yra labai sunkus klausimas. Ar gali kitos organizacijos kibernetinio saugumo kultūros nebuvimas daryti įtaką tavo kibernetiniam saugumui? Manau, kad gali, jei esi susietas su tos organizacijos veikla arba ji yra tavo įrangos ar paslaugų tiekėjas. Jei su kuo nors bendradarbiauji, siunti kokius nors duomenis ar esi sujungęs sistemas tarpusavyje, tai tuomet žinoma, kad kitos organizacijos kibernetinio saugumo lygis tave veiks tiesiogiai. Organizacija, norėdama su kuo nors bendradarbiauti, gali reikalauti laikytis tam tikrų reikalavimų, nors tas partneris greičiausiai turi suvokti, kad, jei jo saugumas yra aukštas, tai jis atrodo patikimiau. Dabar yra taip, kad geras kibernetinis saugumas organizacijoje

yra laikomas gerų manierų ir patikimumo požymiu, o tai jau yra privalumas.“ (1E, asmeninis interviu, 2019-09-12). 3E ekspertas, pateikdamas atsakymą į užduotą klausimą, atsakė, kad „... organizacija vienareikšmiškai gali reikalauti, tiksliau privalo reikalauti, kad jos partneriai adekvačiai vertintų kibernetinio saugumo problemas bei naudotų priemones saugumui užtikrinti.“ (3E, asmeninis interviu, 2019-09-17). Analogiškos nuomonės asmeninio interviu metu laikėsi 2E, 7E, 8E ir 9E ekspertai, kurie pastebėjo, kad kibernetinio saugumo srityje partnerio saugumas yra labai svarbus, kadangi „... žinojimas apie sujungimo su partneriu saugumą ir grėsmių eliminavimas šiame segmente automatiškai sumažins tavo apkrovimą, sprendžiant incidentus“ (2E, asmeninis interviu, 2019-09-14), „...ir galima kalbėti apie partnerio saugumą ne tik šios dimensijos priemonių panaudojimo ribose, bet apie viso kibernetinio saugumo užtikrinimo priemonių spektrą“ (8E, asmeninis interviu, 2019-10-14), kadangi „... būtent pasitikėjimas vienas kitu ir komandinis darbas kibernetinio saugumo užtikrinimo kontekste leidžia visiems būti atsparesniems“ (7E, asmeninis interviu, 2019-10-05), „... labiau apsaugotiems ir galintiems vieningai priešintis galimiems ateities incidentams.“ (9E, asmeninis interviu, 2019-10-17);

2. Organizacijos *partnerių kibernetinis saugumas visiškai nedaro įtakos* pačios *organizacijos* kibernetiniam saugumui, kadangi apsaugota organizacija, kurioje kibernetinio saugumo užtikrinimas yra pasiekęs tam tikrą išsivystymo lygį, yra praktiškai atspari visoms ją supančioms grėsmėms. Tokios nuomonės laikėsi 4E ekspertas, kuris sakė, kad „... organizacijai pasiekus tam tikra kibernetinio saugumo užtikrinimo lygmenį bei atsparumą ją supančioms grėsmėms, beveik nesvarbu, koks yra tavo partnerių ar paslaugų tiekėjų kibernetinio saugumo lygmuo. Pasinaudodamas technologijomis, tu gali aiškiai nusistatyti, kokius duomenis persiųsi partneriams, taip pat kokius prisijungimus prie savo sistemų toleruosi. Žinoma, turi turėti suvokimą, ką norėtum rezultate gauti, bet tai tik patirties reikalas. Nemanau, kad organizacijai, kuri tau teikia paslaugas ar duomenis, labai svarbus saugumo buvimas. Viską gali išspręsti savo pusėje, o partnerių saugumas – tai yra jų reikalas. Nemanau, kad tai turi būti kažkoks esminis klausimas, apsprendžiantis partnerystės ar bendradarbiavimo galimybes.“ (4E, asmeninis interviu, 2019-09-23);
3. Organizacijos *partnerystės klausimai* turi būti *sprendžiami, nagrinėjant* galimų partnerių *kibernetinio saugumo užtikrinimą individualiai*. Pasak 5E ir 6E ekspertų, kurie pažymėjo, kad „... būtent tokios, pavadinkime diplomatinės, pozicijos savo veikloje privalo laikytis organizacija. Reikia įsivertinti savo kibernetinį saugumą, įvertinti partnerius ir nuspręsti, ar bendradarbiavimas ir infrastruktūros sąlyčio taškai nepadidins tau grėsmių. Žinoma, kad būtų puiku, jei tavo partneris turėtų tokį patį saugumą, kaip ir tu, bet ne visada tai yra įmanoma“ (5E, asmeninis interviu, 2019-09-27), kadangi „... tai priklauso nuo daugelio dalykų: partnerio finansavimas, situacijos suvokimas, tavo reikalavimai, finale – nuo ekonominio pagrįstumo paskaičiavimo. Gali būti, kad verčiau susijungti tinklais su tuo, kuris mažiau saugus ir mokėti mažiau, nei su tuo, kuris yra daug investavęs

į saugą ir prašo kosminių paslaugų kainų. Gal verčiau tuos pinigus skirti savo apsaugos padidinimui? Gal iš to bus daugiau naudos? Manau, kad kiekvienas atvejis yra individualus ir kiekvieną situaciją reikia spręsti atskirai.“ (6E, asmeninis interviu, 2019-10-05).

Apibendrinant ekspertų atsakymus į empirinio tyrimo klausimus, susijusius su kibernetinio saugumo kultūros dimensijos įtaka organizacijos kibernetinio saugumo valdymo įgyvendinimu, galima teigti, kad saugumo kultūros problematika organizacijoje yra labai aktuali ir gali būti laikoma vienu iš aspektų, galinčiu stipriai veikti visos organizacijos kibernetinį saugumą. Šis faktas patvirtina pasaulio mokslininkų ir kibernetinio saugumo ekspertų išsakytas nuomones, kad organizacijos pažeidžiamumas priklauso nuo organizacijos narių pažeidžiamumo (Solms ir Solms, 2009; Deighton, 2015; Štitilis, Klišauskas, 2015; Limba ir kt., 2017; Šarkūnas, 2017; James, 2018; Riddle, 2019). Tačiau nėra taip paprasta identifikuoti, kuri iš organizacijos narių grupių yra labiausiai pažeidžiama ir mažiausiai atspari kibernetinio saugumo incidentams. Saugumo ekspertai, pasaulio mokslininkai ir kibernetinio saugumo produktų gamintojai, vertindami kibernetines grėsmes, vieningai tvirtina, kad pagrindiniu aspektu, darančiu įtaką organizacijos saugumui, turi būti laikomas žmogiškasis faktorius, t.y. personalo pažeidžiamumas, neišskiriant tam tikros šio personalo rolės organizacijos veikloje. Būtent personalo pažeidžiamumas buvo įvardijamas pagrindine saugumo problema pasaulio mokslininkų ir kibernetinio saugumo organizacijų tyrimuose (Techrepublic, 2004; Wei ir kt., 2010; Trim, Lee, 2014; Deighton, 2015; Latham & Watkins, 2016). Personalo ugdymas, organizacijos kultūros ir vertybių puoselėjimas, kibernetinio saugumo kontekste gali užtikrinti sklandų saugumo kultūros dimensijos įgyvendinimą organizacijos kibernetinio saugumo valdyme.

Tyrimo dalyviai, vertindami organizacijos veiksmus ir priemones, kurios gali būti panaudojamos kibernetinio saugumo kultūros dimensijai įgyvendinti, pažymėjo, kad sklandžiam sistemos veikimui reikalinga vertinti kiekvieną organizaciją individualiai, atsižvelgiant į jos dydį, darbo specifiką, atstovaujamą sektorių bei skiriamą finansavimą. Tačiau visi šie aspektai gali veikti tik gerinimo priemonių panaudojimo mąstą, bet ne jų panaudojimo būtinumą. Siekiant puoselėti kibernetinio saugumo vertybes, yra būtina: nustatyti ar paskirti atsakingus darbuotojus, išanalizuoti problemines sritis, nustatyti gerinimo galimybes, numatyti vizijas, pasirengti veiklos planus, juos įgyvendinti bei vykdyti periodinį visų anksčiau paminėtų priemonių vertinimą ir, jei būtina, koregavimą.

3.1.5. Technologinio saugumo įtaka kibernetiniam saugumui

Empirinio tyrimo metu ekspertams taip pat buvo užduodami klausimai, susiję su technologinio saugumo faktoriaus įtaka kibernetinio saugumo valdymui organizacijoje. Dažnai technologinis aspektas ir technologinė bei programinė įranga yra traktuojama kaip vienintelė priemonė, kuria yra įmanoma užtikrinti kibernetinį saugumą. Tačiau pažymėtina, kad pasaulio mokslininkai, politikai, kibernetinio saugumo produktų gamintojai ir įvairios organizacijos vis dažniau akcentuoja, kad vien tik technologijos yra bejėgės kovoti su dabartiniais kibernetinio saugumo incidentais.

Šiame disertaciniame darbe siūlomo kibernetinio saugumo valdymo modelio technologinio kibernetinio saugumo dimensija yra nagrinėjama technologiškai neutraliu požiūriu, akcentuojant tik technologinių saugumo priemonių valdymo kontekstą. Manytina, kad toks požiūris į technologinio saugumo dedamąją kibernetinio saugumo kontekste suteikia disertaciniame darbe siūlomam kibernetinio saugumo valdymo modeliui galimybę išlikti technologiškai neutraliu, tokiu būdu apsaugant nuo nereikalingų diskusijų, atsirandančių technologinių priemonių panaudojimo efektyvumo bei tinkamumo vertinimo plotmėje.

Nagrinėjant kibernetinio saugumo ekspertų atsakymus apie technologinį kibernetinį saugumą, pastebėtina, kad visi ekspertai vienbalsiai pareiškė, kad technologinio saugumo dimensijos įgyvendinimas organizacijoje vienareikšmiškai reikalingas ir be technologinių priemonių įgyvendinimo, kaip vienos iš kibernetinio saugumo komponentų, neverta tikėtis kibernetinio saugumo organizacijoje. Pažymėtina, kad pats technologinis kibernetinis saugumas ekspertų yra vertinamas skirtingai: dalis ekspertų technologinį saugumą vertina per techninės ir programinės įrangos panaudojimo efektyvumą bei įrangos vykdomas funkcijas; kiti ekspertai, atsakydami į pateiktus klausimus, vertina technologinės įrangos valdymo būtinumą organizacijoje, siekiant išlaikyti šios įrangos veiklos tęstinumą ir vykdomų funkcijų užtikrinimą. Apibendrinus ekspertų pateiktas nuomones, galima išskirti dvejopą požiūrį į technologinio kibernetinio saugumo dimensiją, kai technologinis kibernetinis saugumas:

1. traktuojamas kaip pagrindinių *techninės ir programinės įrangos produktų rinkinys, kuris užtikrina* organizacijos valdomos *infrastruktūros* siūlomų informacinių ir duomenų perdavimo *paslaugų teikimą* vartotojams. 4E ekspertas, apibūdindamas technologinio kibernetinio saugumo dimensiją, pažymėjo, kad „... ši dimensija turi būti suprantama kaip visos adekvačios technologinio saugumo priemonės, kurių panaudojimas mažina infrastruktūros pažeidžiamumą. Tai yra ir programinė įranga, ir maršrutizatoriai, ir ugniasienės, ir dar daug kitokių sprendimų, kurie gali padėti apsisaugoti. Galima naudoti viską, bet reikia, visų pirma, vertinti naudojamos įrangos kainą ir jos nešamą naudą. Nereikia prisipirkti brangių „žaislų“, nes jie gali neduoti naudos, o finansai jau bus išleisti. Apsaugos priemonių sukūrimas yra ne kas kita, kaip technologinių sprendimų tarpusavyje derinimas ir inžinerinių sprendimų paieška, o jei kalbam apie tų technologijų valdymą, tai tas valdymas priklauso tik nuo inžinerinės minties ir sprendimo, kaip tu apsisaugosi. Šiame žingsnyje gali padėti tik technologiniai reglamentai ir standartai, kurie nurodo protokolų ir techninės infrastruktūros suderinamumą bei kurių naudojimas yra privalomas.“ (4E, asmeninis interviu, 2019-09-23). Panašios nuomonės laikėsi ir 5E ekspertas, pažymėdamas, kad „... įgyvendinant technologinį kibernetinį saugumą, svarbus yra tinklo monitoringas, OS nuolatinis atnaujinimas, antivirusinių programų įdiegimas, tinklo sensorių, ugniasienių ir kitų saugos priemonių panaudojimas. Žinoma, tam, kad galima būtų naudoti įrangą, reikia suprasti, kokios jos reikia. Žinoma, yra tam tikri šios srities valdymo standartai, tačiau manau, kad tie standartai nėra būtini, o daug svarbesnis yra supratimas, kokios įrangos reikia. Pasižiūri,

ką gamina, nusimatai, ko reikia, nusiperki ir įdiegi.“ (5E, asmeninis interviu, 2019-09-27);

2. suprantamas kaip *technologinių saugumo priemonių*, skirtų kibernetiniam saugumui organizacijoje užtikrinti, *valdymas*, apimantis technologinės įrangos panaudojimo parinkimą, įsigijimo tikslingumo įvertinimą, įrangos gyvavimo ciklo palaikymą ir kt. 3E ekspertas, atsakydamas į pateiktus klausimus, pažymėjo, kad „... kibernetinio saugumo sprendimai yra tam ir sukurti, kad apsaugotų infrastruktūrą, bet nereikia pamiršti ir tų priemonių administravimo, gal net sakyčiau, kad labiau tinka žodis „valdymo“. Tu privalai ne tik pirkti įrangą, bet ir mąstyti, kokia ji turi būti ir ką ji turi apsaugoti. Pavyzdžiui panagrinėkime ITIL kursą ar dar kažkokį informacinių technologijų ir išteklių valdymo kursą. Techninės įrangos panaudojimas ir konkretus įrangos parinkimas ten kažkodėl neaptariamas. Tai tik sudedamoji dalis nuo didelio standartizuoto proceso, nuo rekomendacijų. O visi standartai ir rekomendacijos nėra laisvalaikio skaitiniai, jas kūrė savo srities profesionalai, todėl, mano manymu, yra būtina vadovautis šiais dokumentais. Tačiau tik būtinais, o ne visais įmanomais ar pertekliniais, kas irgi yra svarbu. Planuodamas technologijų panaudojimą, turi, visų pirma, žinoti, kokiam tikslui to reikia ir kaip tu tą tikslą pasieksi, o kokias sistemas pastatysi – šiame etape nelabai svarbu.“ (3E, asmeninis interviu, 2019-09-17). Analogiškos pozicijos laikėsi visi kiti empiriniame tyrime dalyvavę kibernetinio saugumo ekspertai, kurie, atsakydami į jiems pateiktus klausimus, pažymėjo, kad „... technologinio kibernetinio saugumo įgyvendinimą organizacijoje reikia vertinti ne iš inžinieriaus pusės. Turbūt pasibaigė laikai, kai kibernetinis saugumas buvo vien tik „protingų dėžučių“ programavimo ir technologinių priemonių įdiegimo kompiuteriniame tinkle menas, siekiant užtikrinti informacinių sistemų teikiamų paslaugų įgyvendinimą. Svarbiausia yra valdymas, jis yra būtinybė ir be jo nieko nepadarysi“ (1E, asmeninis interviu, 2019-09-12), „... technologijos saugumo užtikrinimo procese turi būti suprantamos ne kaip kertinis akmuo, o kaip įrankis, kuris privalo būti valdomas kaip ir bet kuris kitas turtas. Kitais žodžiais kalbant, tai turi būti suprantama kaip transporto valdymas, personalo vadyba, planavimo ir valdymo proceso įgyvendinimas. Paprastas valdymo procesas, kuris užtikrina šių priemonių panaudojimą, gyvenimo ciklo stebėjimą, išlaikymą ir kt. Yra aibė metodikų ir rekomendacijų, kaip tai galima atlikti. Krūva standartų, kuriuos gali prisitaikyti, adaptuoti ir naudoti savo veiklai organizuoti. Žinoma, tie standartai turi būti adaptuojami pagal kiekvieną organizaciją, bet esminiai principai išlieka tie patys. Naudodamas standartus, tu sureguliuoji ir nusimatai visą procesą, įsivertini visas savo galimybes, o kokia bus įranga – visiškai nesvarbu. Nereikia galvoti, kad, nusimačius vieno ar kito gamintojo konkrečią įrangą, tavo saugumas bus didesnis. Jei neišmoksi tinkamai susireguliuoti procesus, nieko gero nesigaus.“ (2E, asmeninis interviu, 2019-09-14). 6E ekspertas pažymėjo, kad „... technologinių ir inžinierinių sprendimų derinimas, negalvojant apie tų sprendimų valdymo procesą, yra bandymas „statyti vežimą prieš arklį“. Du dešimtmečius atgal tai gal ir buvo įmanoma, bet dabar mes turim pakankamai daug IT specialistų, kurie

išmano savo darbą ir sugeba ganėtinai neblogai tvarkytis su kibernetinio saugumo iššūkiais. Tačiau atsiranda vienas aspektas, kurio dažnai neįvertinam. Vienas ar du specialistai gali susitarti, gali rasti tam tikrą bendrą vardiklį, bet kai specialistų atsiranda daugiau, organizacija pradeda panašėti į „bandymų institutą“, kuriame mokslininkai atlieka eksperimentus, siekdami kibernetinio saugumo užtikrinimo. Teko matyti, kaip po tokių eksperimentų likdavo brangi techninė ir programinė įranga, kurios niekas naudoti nebenorėjo, nes kitas įrenginys, nupirktas tuo pačiu metu, sugeba atlikti tas pačias funkcijas. Valdymo sistemos įvedimas ir jos viršenybė virš technologinių sprendimų, užtikrina tokių nesusipratimų eliminavimą. Valdymas, planavimas, analizė ir tų procesų reglamentavimas technologijų srityje padeda taupyti pinigus ir skatina mąstyti, pasinaudojant principu *out-of-the-box*.“ (6E, asmeninis interviu, 2019-10-05). 7E ekspertas, atsakydamas į pateiktus klausimus, pareiškė, kad „... technologinio kibernetinio saugumo laikai jau pasibaigė. Žinoma, nereikia suprasti tiesiogiai ir nustoti naudotis incidentų prevencijos sistemomis. Tas technologinis saugumas dabar jau slepiasi valdymo šešėlyje. Dabar turbūt valdymas yra svarbiau už technologijas“ (7E, asmeninis interviu, 2019-10-05), ir „... visiškai nesvarbu, kokia yra priemonė, svarbu, kodėl tu nusprendei, kad ji tau reikalinga ir kodėl ji gali tave apsaugoti? Analizė ir planavimas gali duoti atsakymus į klausimus, ko tu nori ir kaip tai pasiekti, o technologijos lieka antrame plane.“ (8E, asmeninis interviu, 2019-10-14). „Baigėsi tie laikai, kai IT departamentas pats priiminėjo sprendimus, kokia įranga jiems reikalinga. Dabar IT vadovas turi būti inžinierius su gerais vadybininko įgūdžiais. Neužtenka būti tik technologinių procesų ar įrangos žinovu, būtina būti geru administratoriumi, gebėti planuoti ir numatyti kas ir kaip bus po trijų ar penkerių metų. Žinoti kaip bus, o priemonių reikalingų planams įgyvendinti visuomet atsiras.“ (9E, asmeninis interviu, 2019-10-17).

Pažymėtina, kad dauguma kibernetinio saugumo ekspertų, dalyvavusių empiriniame tyrime, pažymi, kad požiūris į technologinį kibernetinį saugumą šiuolaikiniame kontekste turi būti keičiamas, pereinant nuo konkrečių inžinerinių sprendimų dėl technologinės įrangos suderinamumo ir naudojimo naudingumo įvertinimo link technologinių sprendimų valdymo aspektų įgyvendinimo organizacijoje nagrinėjimo. Technologijų valdymo procesas, kuris sujungia savyje analizės, sumanymo, įgyvendinimo ir kontrolės mechanizmus, turi būti esminiu technologinio saugumo užtikrinimo mechanizmu, inkorporuojančiu į save inžinierinius sprendimus. Pasak daugumos ekspertų, būtent toks organizacijos požiūris į technologinio saugumo dedamąją kibernetinio saugumo valdymo kontekste suteikia didžiausią pridėtinę vertę ir galimybes, taupant organizacijos turimus išteklius, pasiekti labiausiai apčiuopiamą rezultatą. Tokia nuomonė taip pat išreiškia ir pasaulio mokslininkai bei tarptautinės organizacijos, tvirtindamos, kad kibernetinis saugumas yra ne tik technologinis požiūris į organizacijos išteklių saugumą (Cayirci, Ghergherehchi, 2011; Solms, Niekerk, 2013; Campbell, 2017; Collier, 2018; E&Y, 2018).

Tyrime dalyvavę ekspertais taip pat buvo klausiami apie technologinio kibernetinio saugumo priemonių ir procesų įgyvendinimą organizacijoje. Apibendrinus atsaky-

mus, galima teigti, kad organizacijai, siekiančiai tinkamai įgyvendinti technologinio kibernetinio saugumo dimensiją, būtina: identifikuoti organizacijos veikloje naudojamas technologines priemones; išsiaiškinti šių priemonių pažeidžiamumą; nustatyti ir įvertinti saugumo užtikrinimo priemonių naudojimo tikslingumą; parengti ir įgyvendinti technologinio saugumo valdymo planą; atlikti plano įgyvendinimo vertinimą bei atlikti galimas plano korekcijas. Ekspertų nuomonė ir pateikti komentarai dėl siūlomo valdymo modelio technologinio kibernetinio saugumo dimensijos bus įvertinti ir panaudoti, tikslinant kibernetinio saugumo valdymo modelio struktūrą.

3.1.6. Rizikos valdymo įtaka kibernetiniam saugumui

Vykdant empirinį tyrimą, ekspertai buvo apklausiami apie rizikos valdymo dimensijos svarbą kibernetinio saugumo kontekste. Atliekant ekspertų pateiktų atsakymų analizę, galima pastebėti, kad visi ekspertai vienareikšmiškai nurodo rizikos valdymo dimensijos svarbą kibernetinio saugumo valdymo procese. Rizikos valdymas daugumos ekspertų buvo įvardijamas kaip svarbiausias (*esminis, pamatinis, kertinis*) kibernetinio saugumo valdymo įgyvendinimo procesas organizacijoje.

1E ekspertas, atsakydamas į klausimus dėl rizikos valdymo dimensijos būtinumo kibernetinio saugumo valdymo kontekste, pažymėjo, kad „... tai yra sudedamoji dalis saugumo, čia gal net pirmas žingsnis kibernetiniame saugume. Nesvarbu, per kokią prizmę žiūrėtum, bet pirmiausia įsivertini rizikas, o po to jau sprendi, ką reikia pirmiausiai apsaugot. Turbūt visų modelio dimensijų pamatas yra rizikos analizė, na jei ir ne visų, tai didžiosios daugumos. Vienareikšmiškai visko apsaugoti yra neįmanoma, tai privalu koncentruotis į ten, kur yra didžiausios rizikos. Įvardini rizikas, padarai visą rizikos analizę ir tuomet žiūri, kokios priemonės gali būti naudojamos konkrečiai rizikai sumažinti. Bet reikia suprasti, kad nebūtinai reikia naudoti technologines priemones, gali rizikas sumažinti ir kitaip. Reikia vertinti kiekvieną riziką atskirai ir spręsti, kas naudingiau: ar nupirkti technologinę priemonę, ar pasinaudoti kokiais nors kitais suvaldymo mechanizmais. Pažiūrėjęs į siūlomą modelį, galiu pasakyti, kad rizikos vertinimo aspektai yra kiekvienoje dimensijoje. Galima, žinoma, šias dimensijas įgyvendinti ir be rizikos vertinimo, bet naudingiau, geresnis rezultatas bus, iškarto vertinant galimas dimensijų rizikas. Rizikos valdymo procesas mažina kaštus ir daro kibernetinio saugumo valdymą naudingesnį bei labiau orientuotą į rezultatą, o ne į patį procesą.“ (1E, asmeninis interviu, 2019-09-12). 6E ekspertas, kalbėdamas apie rizikos valdymą, pareiškė, kad „... tik visiškas neišmanymas, atsilikimas, saugumo ignoravimas, saugumo kultūros nebuvimas, ypač tarp vadovaujančių, sprendimus priimančių žmonių, gali priversti kibernetinio saugumo valdymą organizacijoje vykdyti, neatsižvelgiant į rizikos valdymo aspektus.“ (6E, asmeninis interviu, 2019-10-05). Analogiškas nuomones pateikė ir visi kiti empiriniame tyrime dalyvavę kibernetinio saugumo ekspertai.

Apibendrinant tyrime dalyvavusių ekspertų atsakymus, galima teigti, kad kibernetinio saugumo valdymo kontekste rizikų valdymo proceso elementų galima atrasti bet kuriame kibernetinio saugumo valdymo užtikrinimo etape. Pasak ekspertų, „... labai dažnai galima pamatyti, kad rizikos valdymas organizacijoje yra vykdomas, net

nesuvokiant (nesugebant įvardyti) šio proceso. Kiekviena organizacija, stengdamasi apsaugoti savo išteklius ir planuodama technologinių priemonių įsigijimą, vienaip ar kitaip vykdo rizikos analizę: identifikuoja galimas grėsmes, nustato jų pavojingumo lygį, numato šių grėsmių šalinimo priemones. Tai faktiškai yra labai artimas procesas rizikos valdymui. Žinoma, šio proceso rezultatas yra diskutuotinas. Tačiau nemanau, kad organizacija gali vienareikšmiškai pasakyti, kad jos padaryti sprendimai ir nupirktos technologijos yra pakankamai geras atsakas į identifikuotą riziką.“ (2E, asmeninis interviu, 2019-09-14). „Organizacijai turbūt reikia suvokti, kad rizikos valdymo specialisto parengimas ir šių funkcijų dedikavimas jam gali palengvinti visos organizacijos darbą, sutaupyti lėšas ir išvengti nemalonių pasekmių dėl netinkamų sprendimų. Žinoma, rizikos valdymo profesionalas reikalingas, bet reikia įvertinti organizacijos veiklą, jos poreikius ir dydį. Viskas yra labai subtilu ir priklauso nuo tam tikros situacijos.“ (7E, asmeninis interviu, 2019-10-05).

Daugumą ekspertų taip pat pažymėjo, kad rizikos valdymas iš esmės yra labai sudėtingas ir ilgai trunkantis procesas, tačiau jo vykdymas yra būtinas šiuolaikinėje organizacijoje. Būtent rizikos valdymas suteikia galimybę sumažinti kibernetinio saugumo incidentų padarinius, kaip tai pažymi mokslininkai (Deighton, 2015; Latham & Watkins, 2016; Vega ir kt., 2017; Patiño ir kt., 2018). Ekspertai taip pat pažymėjo, kad egzistuoja nemažai rizikos valdymo standartų ir metodikų, kurios gali būti panaudojamos rizikos valdymo proceso metu, tačiau vienas iš patogiausių instrumentų, supaprastinančių rizikų valdymo proceso įgyvendinimą organizacijoje, yra specializuotos rizikos analizės vertinimo programinės įrangos panaudojimas. Taip pat pastebėtina, kad ekspertai kaip vieną iš būtiniausių rizikos analizės proceso įgyvendinimo organizacijoje sąlygų įvardino organizacijos vadovų visapusišką palaikymą.

Ekspertai akcentavo, kad, siekiant sėkmingo rizikos valdymo dimensijos įgyvendinimo organizacijoje, yra būtina atlikti šiuos (minimalius) žingsnius: nustatyti rizikos valdymo proceso ypatumus; atlikti galimų rizikų vertinimą, jų analizę ir klasifikavimą; parengti rizikų valdymo planą; vykdyti planą bei vertinti organizacijos veiksmų atitikimą parengtam planui. Pastebėtina, kad ekspertai taip pat akcentavo, kad rizikų valdymo procesas privalo būti vykdomas tam tikru ciklišku (yra tęstinis), kadangi tik taip yra įmanoma stebėti pokyčius rizikos valdymo dimensijoje.

3.1.7. Kibernetinių incidentų valdymo įtaka kibernetiniam saugumui

Ekspertinio interviu metu kibernetinio saugumo ekspertams buvo užduodami klausimai, susiję su kibernetinių incidentų valdymo dimensijos įtaka kibernetinio saugumo valdymo procese. Pažymėtina, kad būtent šios dimensijos kontekste sprendžiamų kibernetinių incidentų valdymo rezultatai dažniausiai yra identifikuojami kaip kibernetinio saugumo įvertinimas.

Atkreiptinas dėmesys, kad, analizuojant kibernetinio saugumo ekspertų atsakymus apie kibernetinių incidentų valdymą, galima teigti, kad visi ekspertai įvardijo šią dimensiją kaip vienareikšmiškai svarbią kibernetinio saugumo užtikrinimo kontekste, tačiau ekspertų požiūrį į kibernetinių incidentų valdymą galima suskirstyti į dvi grupes, kai kibernetinių incidentų valdymas yra suprantamas kaip:

1. organizacijos *galimybė tinkamai reaguoti ir pasipriešinti* kibernetinio saugumo incidentui, aptikus jį organizacijos valdomose informaciniuose ištekliuose. 4E ekspertas pažymėjo, kad „... tinkamai pasiruošti kibernetinių incidentų valdymui turbūt nėra įmanoma. Nežinai iš tikrųjų, kurioje vietoje atsiras pažeidžiamumas ir kada jis bus išnaudotas, o bandyti prognozuoti galimus incidentus turbūt nelabai įmanoma. Tik tinkamas pasirengimas ir greita reakcija į pastebėtą ataką tinkle arba laiku aptiktas virusas gali sumažinti padarinius.“ (4E, asmeninis interviu, 2019-09-23). Panašią nuomonę buvo išsakęs ir 5E ekspertas: „... incidentų valdymas labiau susijęs su reakcija, su tavo galimybėmis lokalizuoti incidentą ir išvengti didelės žalos. Žinoma, galima sakyti, kad instrukcijos darbuotojams, numatančios jų veiksmus, yra incidentų valdymo dalis, bet aš sakyčiau, kad instrukcijos ne visuomet gali viską numatyti. Mano patirtis labiau priartėja prie reagavimo į incidentus koncepcijos, nors čia yra kaip ir su informacijos saugumo sąvokos kaita, vieną dieną ima ir pasikeičia“ (5E, asmeninis interviu, 2019-09-27);
2. organizacijos *galimybė prognozuoti galimus kibernetinius incidentus, taip pat aptikti, suvaldyti bei efektyviai priešintis* vykstantiems ar atsirandantiems *kibernetiniams incidentams*. Būtent šios nuomonės laikėsi didžioji dauguma ekspertų, pateikdami savo atsakymus apie kibernetinių incidentų valdymo dimensiją. Atsakydamas 1E ekspertas akcentavo, kad „... incidentų valdymas nėra vien tik reagavimas į vykstančią kibernetinę ataką. Vienareikšmiškai incidentų valdymas yra šiek tiek daugiau nei tik reakcija į jau konstatuotus faktus, kad tave kažkas užpuolė. Supraskime kibernetinių incidentų valdymą kaip tam tikrą strategiją, kurios pagrindinis tikslas yra atgrasyti priešą. Bet, siekdamas atgrasyti, tu galvoji ir apie tai, kokių veiksmų reikia imtis, vykdai žvalgybą, stiprini savo pajėgas ir dedi visas pastangas patobulėti ten, kur priešas yra stiprus. Taip yra ir su incidentais. Turi analizuoti aplinką, žiūrėti į incidentus aplink save, vertinti visas smulkmenas. Tik tuomet galėsi užsitikrinti saugumą.“ (1E, asmeninis interviu, 2019-09-12). Panašią nuomonę išreiškė ir likusieji tyrime dalyvavę kibernetinio saugumo ekspertai, pažymėdami, kad „... kibernetinių incidentų valdymas negali būti tik atsakas, tai ir prognozės, ir bendradarbiavimas ir mokymasis iš kitų“ (2E, asmeninis interviu, 2019-09-14), o „...kalbant apie reagavimą į incidentus ar į dalykus, kuriuos pastebėjai vykstant tavo kompiuteriniame tinkle, tai čia yra tiesiog viena iš kibernetinių incidentų valdymo dimensijos sudedamųjų dalių.“ (3E, asmeninis interviu, 2019-09-17).

Apibendrinant ekspertų nuomones apie kibernetinio saugumo incidentų valdymo reiškinį, galima teigti, kad šią sąvoką dauguma ekspertų supranta ne tik kaip bandymą atstatyti normalų informacinių išteklių veikimą po kibernetinio incidento, bet ir kaip galimybę visiškai išvengti galimų kibernetinio saugumo incidentų atsiradimo organizacijos infrastruktūroje, tam tikslui pasinaudojant visomis įmanomomis priemonėmis. Tik kompleksiškas požiūris į galimų incidentų atsiradimą, jų prognozavimas, jau įvykusių incidentų analizė ir kitos kibernetinio saugumo valdymo priemonės gali sudaryti tinkamas sąlygas incidentams valdyti. Tyrimo metu taip pat buvo patvirtintos pasaulio

mokslininkų ir kibernetinio saugumo organizacijų pateiktos nuomonės, kad organizacijai yra būtina turėti specialius planus ir taisykles, siekiant valdyti kibernetines grėsmes (Deighton, 2015; Latham & Watkins, 2016; Limba ir kt., 2017; Walker, 2018).

Atlikus ekspertų pateiktų atsakymų apie kibernetinių incidentų valdymo dimensijos priemonių įgyvendinimą analizę, galima teigti, kad organizacija, siekdama tinkamai vykdyti kibernetinių incidentų valdymą, privalo: suformuoti incidentų valdymo komandas, nustatyti incidentų valdymo proceso ypatumus, parengti veiklos instrukcijas ir reagavimo į incidentus planą, vykdyti atsaką į incidentus bei kaupti informaciją, kurią galės naudoti pasikartojantiems incidentams spręsti. Visos šioje tyrimo dalyje pateiktos ekspertų rekomendacijos bus panaudotos, tikslinant siūlomą kibernetinio saugumo modelio struktūrą.

3.1.8. Kibernetinio saugumo valdymo modelio panaudojimas Lietuvos elektroninių rinkimų sistemai sukurti

Empirinio tyrimo pabaigoje kibernetinio saugumo ekspertams buvo užduodami klausimai, susiję su siūlomo kibernetinio saugumo valdymo modelio panaudojimo galimybėmis, siekiant Lietuvoje įgyvendinti elektroninius rinkimus. Taip pat buvo klausima, kokios organizacijos galėtų būti įtrauktos į Lietuvos elektroninių rinkimų sistemos kūrimo procesą.

Pastebėtina, kad visi ekspertai, atsakydami į klausimą dėl modelio tinkamumo, vienareikšmiškai sutiko, kad modelis yra tinkamas elektroninių rinkimų sistemai įgyvendinti. 2E ekspertas sakė: „... manau, kad siūlomas kibernetinio saugumo valdymo modelis yra teisingas, kadangi apima visas įsivaizduojamas kibernetinio saugumo projekcijas, kuriose gali kilti saugumo pažeidžiamumo grėsmės. Papildomos net negalėčiau įvardyti. Manau, kad modelis gali būti naudojamas ne tik rinkimams apsaugoti, bet ir kitose organizacijose, kurios galvoja apie tai, kaip išlikti saugiomis šiame grėsmingame pasaulyje. Galvoju, kad kompleksiškas požiūris yra labai geras dalykas, nes neįmanoma užtikrinti kibernetinio saugumo vienoje srityje. Su išlyga galima sakyti, kad, jei tu nieko neturi, tai tu gali žiūrėti vien tik į technologinį aspektą: pasistatyti ugniasienę ir pasakyti, kad mes tapom technologiškai saugesni. Jeigu tu esi įžengęs į kibernetinio saugumo kultūros kūrimo lygmenį, rizikos valdymo klausimų sprendimą, tai galimas tik kompleksinis požiūris, nes kiekvienas pokytis iššaukia būtinumą nagrinėti jo įtaką kitoms tavo kontroliuojamoms sritims. Gali imtis tam tikrų atskirų sričių gerinimo priemonių, bet kažkada ateis tas momentas, kai reikės sujungti jas visas į vieną visumą ir žiūrėti bendrą kibernetinio saugumo pokytį. Manau, kad modelį tikrai galima panaudoti elektroninių rinkimų sistemai sukurti ir įgyvendinti Lietuvoje. Reikia tiesiog politinės valios ir noro paskirti atsakingus asmenys, sudaryti didelę darbo grupę, kuri norėtų dirbti. O tuomet, manau, tik laiko klausimas, kada mes galėsime balsuoti kaip Estijos gyventojai.“ (2E, asmeninis interviu, 2019-09-14). Panašią nuomonę išsakė ir 1E ekspertas, pažymėdamas, kad „... įgyvendinant elektroninius rinkimus, būtina įgyvendinti ir kibernetinio saugumo valdymą. Čia net kalbos jokios nėra. Saugumas yra būtinas. O kokį modelį pasirinkti? Na, jų tikrai ne vienas yra: SANS‘o, NIST‘o. Bet jie šiek tiek gal kitokie nei šis siūlomas, labiau į kažkokią

konkrečią sritį orientuoti, į technologijas. Labai įdomiai pasijutau, kai pradėjau žiūrėti siūlomą modelį. Atrodo, kad jis visas įmanomas sritis padengia, bent jau nesugalvoju, ko dar trūksta. Šis modelis tikrai nenusileidžia kitiems. Manau, kad jis tikrai tinkamas elektroniniams rinkimams. Manau, kad ir kitoms sistemoms, siekiant saugos, galima drąsiai jį naudoti.“ (1E, asmeninis interviu, 2019-09-12). Visų kitų tyrime dalyvavusių ekspertų nuomonės apie siūlomą kibernetinio saugumo valdymo modelio įgyvendinimą beveik nesiskyrė nuo 1E ir 2E ekspertų išsakytų nuomonių, tačiau 5 ekspertai pažymėjo, kad yra būtinos tam tikros modelio korekcijos, nes „... modelis turi būti sudarytas pakopomis, turėti lygius, kad būtų supaprastintas jo įgyvendinimas“ (4E, asmeninis interviu, 2019-09-23), kadangi „... įgyvendinti visus pokyčius iškart būtų per daug drąsu. Mano siūlymas būtų – pagalvoti apie dimensijų įgyvendinimą, naudojantis tam tikru ciklišku, pavyzdžiui, „plan-do-act-check“. Sugalvojai, padarei, patikrinai. Ir taip kiekvieną dimensiją.“ (7E, asmeninis interviu, 2019-10-05).

Empirinio tyrimo metu ekspertų buvo prašoma įvardyti Lietuvos institucijas ar organizacijas, kurios turėtų būti įtrauktos į elektroninių rinkimų sistemos įgyvendinimą Lietuvoje. Ekspertai, pateikdami atsakymus, pažymėjo, kad būtina įtraukti visas teisėsaugos, nacionalinio saugumo užtikrinimo institucijas ir organizacijas, pilietinį aktyvumą skatinančias organizacijas, viešojo ir privataus sektoriaus organizacijas, dirbančias su kibernetinio saugumo užtikrinimo sprendimais ir technologijomis, akademinės visuomenės atstovus, masinio informavimo priemones, strateginės komunikacijos specialistus ir kitas organizacijas, kurios gali vienaip ar kitai prisidėti prie kibernetinio saugumo gerinimo per įvairiausias kibernetinio saugumo valdymo ir suvokimo prizmes.

Ekspertai tvirtino, kad vienas iš pagrindinių aspektų kliudančių elektroninių rinkimų sistemų įgyvendinimui Lietuvoje yra susijęs su menku visuomenės informavimu apie elektroninių rinkimų sistemų teikiamą pranašumą, pasitikėjimo sistemomis trūkumu. Visuomenė turi būti geriau informuojama apie elektroninių rinkimų sistemų veikimo principus ir naudojamus saugumo užtikrinimo mechanizmus, tokiu būdu skatinant piliečių pasitikėjimą elektroniniu rinkimu sistema. *Saugios sistemos konstravimas ir visuomenės informavimo didinimas yra vienas esminių aspektų*, galintis sąlygoti piliečių pasitikėjimo elektroninėmis rinkimų sistemomis augimą ir užtikrinantis aktyvesnį piliečių dalyvavimą šalies politiniuose procesuose.

3.1.9. Empirinio tyrimo rezultatai

Atlikus siūlomo kibernetinio saugumo valdymo modelio empirinio tyrimo metu gautų atsakymų analizę bei įvertinus kibernetinio saugumo ekspertų pateiktus siūlymus ir pastebėjimus, susijusius su galimais siūlomo kibernetinio saugumo valdymo modelio patobulinimais, galima suformuluoti šias tyrimo išvadas ir rekomendacijas:

1. Kibernetinis saugumas šiuolaikiniame technologijų pasaulio kontekste, kuriame nė viena diena nėra įsivaizduojama be masinių informavimo priemonių, socialinių tinklų ir elektroninių paslaugų, tampa ne technologinio žinojimo ar inžinerinio meno disciplina, bet reiškiniu, kuris savyje sujungia daugelį šiuolaikinio mokslo sričių ir disciplinų. Tokia empirinio tyrimo išvada patvirtina pasaulio

mokslininkų (Rainer ir kt., 2007; Tisdale, 2015; Limba ir kt., 2017; Štitilis ir kt., 2017; Lackram, Padayachee, 2018; Patiño, Yoo, 2018) atliktų tyrimų rezultatus, pabrėžiant, kad pasaulio evoliucionavimas, technologijų skvarba ir kiti dalykai nulemia naujo požiūrio į kibernetinio saugumo reiškinį atsiradimą, požiūrio, kurio pagrindu tampa labiau valdymo nei technologijų išmanymas;

2. Disertacijos autoriaus siūlomas kibernetinio saugumo valdymo modelis yra tinkamas įvairiapusio kibernetinio saugumo valdymui užtikrinti, kadangi jo struktūroje yra nagrinėjami kibernetinio saugumo valdymo aspektai, susiję su įvairiomis dimensijomis. Toks globalus požiūris į kibernetinio saugumo reiškinį, apimantis galimas grėsmes visuose organizacijos sluoksniuose užtikrina, šiuolaikišką kompleksišką kibernetinio saugumo valdymą, kuris yra akcentuojamas pasaulio mokslininkų ir tarptautinių organizacijų tyrimuose (Limba ir kt., 2017; NATO StratCom COE, 2018; Haynes, 2019; Giniotienė 2019; Sofiou, 2019);
3. Siekiant supaprastinti kibernetinio saugumo valdymo modelio įgyvendinimą, būtina apgalvoti šio modelio suskirstymą į etapus (lygius). Suskirsčius kibernetinio saugumo valdymo dimensijų įgyvendinimą į tam tikrus etapus, atsiras galimybė tinkamai įvertinti organizacijos vykdomų veiksmų tinkamumą kibernetinio saugumo įgyvendinimo kontekste, taip pat sumažins organizacijos galimybes suklysti kibernetinio saugumo valdymo modelio įgyvendinimo metu;
4. Siūlomo kibernetinio saugumo valdymo modelio technologinis neutralumas ekspertų yra vertinamas kaip modelio privalumas, nes jis neįpareigoja organizacijos naudoti konkrečių saugumo sprendimų gamintojų technologinės ir programinės įrangos, kas yra pabrėžiama ir mokslininkų bei valdžios institucijų (LRS, 2014; Papadaki, 2018; Meltzer, 2020). Tokiu būdu organizacijoms yra suteikiama galimybę pačioms įvertinti konkrečių technologinių apsaugos priemonių ir sprendimų panaudojimo tikslingumą kibernetinio saugumo užtikrinimo procese;
5. Įgyvendinant elektroninių rinkimų sistemos kibernetinį saugumą, siūlomas modelis leistų ne tik užtikrinti šios sistemos kibernetinio saugumo valdymą, bet ir sudarytų galimybes kibernetinio saugumo kultūros kūrimo dimensijos priemonėmis informuoti visuomenę apie galimas kibernetinio saugumo grėsmes rinkimų sistemų panaudojimo metu. Taip pat būtų užtikrinta galimybė įtraukti į sistemos kūrimo procesą privataus sektoriaus atstovus, socialiai aktyvias piliečių grupes, akademinę visuomenę ir kt., tokiu būdu ne tik užtikrinant informacijos apie elektroniniu balsavimo sistemų paskirstymą, bet ir kuriant balsavimo sistemos atsparumą tam tikroms kibernetinėms grėsmėms. Ši empirinio tyrimo išvada patvirtina pasaulio mokslininkų darbuose išsakytos nuomonės (Techrepublic, 2004; Wei ir kt., 2010; Singer, Friedman, 2014; Trim, Lee, 2014; Deighton, 2015; WISAC, 2015; Latham & Watkins, 2016; Limba ir kt., 2017);
6. Siūlomas kibernetinio saugumo valdymo modelis turi būti papildytas veiklos vertinimo sistema, kurios panaudojimas yra būtinas, nagrinėjant ir vertinant kiekvienos siūlomo kibernetinio saugumo valdymo modelio dimensijos priemonių įgyvendinimo pasiekimą, taip pat siekiant įvertinti kibernetinio saugumo situacijos pokyčius organizacijoje. Veiklos ir efektyvumo vertinimo sistemos

sukūrimo svarbą organizacijoje taip pat yra pažymėję ir pasaulio mokslininkai (Micheli, Manzoni, 2010; Gomes ir Yasin, 2011; Striteska, Spickova, 2012; Franco-Santosa ir kt., 2012; Striteska, Jelinkova, 2014);

7. Sukurtas kibernetinio saugumo valdymo modelis visapusiškai nagrinėja kibernetinio saugumo užtikrinimo problematiką, suteikdamas modelio naudotojui galimybes, įgyvendinus visas kibernetinio saugumo valdymo modelio dimensijų priemones, priartėti prie visiško teorinio kibernetinio saugumo užtikrinimo organizacijoje.
8. Disertacijos autoriaus sukurtas kibernetinio saugumo valdymo modelis gali būti naudojamas ne tik elektroninių rinkimų sistemų kibernetiniam saugumui užtikrinti. Visiškai įmanomas ir realus yra siūlomo modelio panaudojimas, siekiant įgyvendinti kibernetinio saugumo valdymą bet kokioje viešojo ar privataus sektoriaus organizacijoje. Siekiant įgyvendinti kibernetinio saugumo valdymą organizacijoje, jis gali būti naudojamas kaip tam tikros kibernetinio saugumo valdymo pamatinės gairės, kurių adaptavimas konkrečiai organizacijai prisidės prie šios organizacijos kibernetinio saugumo valdymo gerinimo;

Atsižvelgiant į atlikto empirinio tyrimo metu gautas išvadas ir pateiktas ekspertų nuomones, taip pat teorinių tyrimų metu išnagrinėtas bei atskleistas teorines įžvalgas, disertaciniame darbe toliau yra sukurtas ir nagrinėtas patikslintas kibernetinio saugumo valdymo modelis elektroninių rinkimų įgyvendinimui.

3.2. Patikslinto kibernetinio saugumo valdymo modelio struktūros analizė

Šioje disertacinio darbo dalyje bus atliekama modifikuoto koncepcinio kibernetinio saugumo valdymo modelio, skirto elektroniniams rinkimams įgyvendinti, struktūros analizė, pateikiant rekomendacijas ir pasiūlymus, kokios kibernetinio saugumo valdymo priemonės turi būti naudojamos, įgyvendinant kibernetinio saugumo valdymo modelio dimensijas, atsižvelgiant į tyrimo metų gautus duomenis. Pažymėtina, kad, aptariant kibernetinio saugumo valdymo modelio struktūrą disertaciniame darbe, nėra nagrinėjami konkretūs technologiniai sprendimai, techninė ir programinė įranga ir priemonės, kurios yra naudojamos kibernetinio saugumo užtikrinimo procese, bei šių priemonių taikymo efektyvumas.

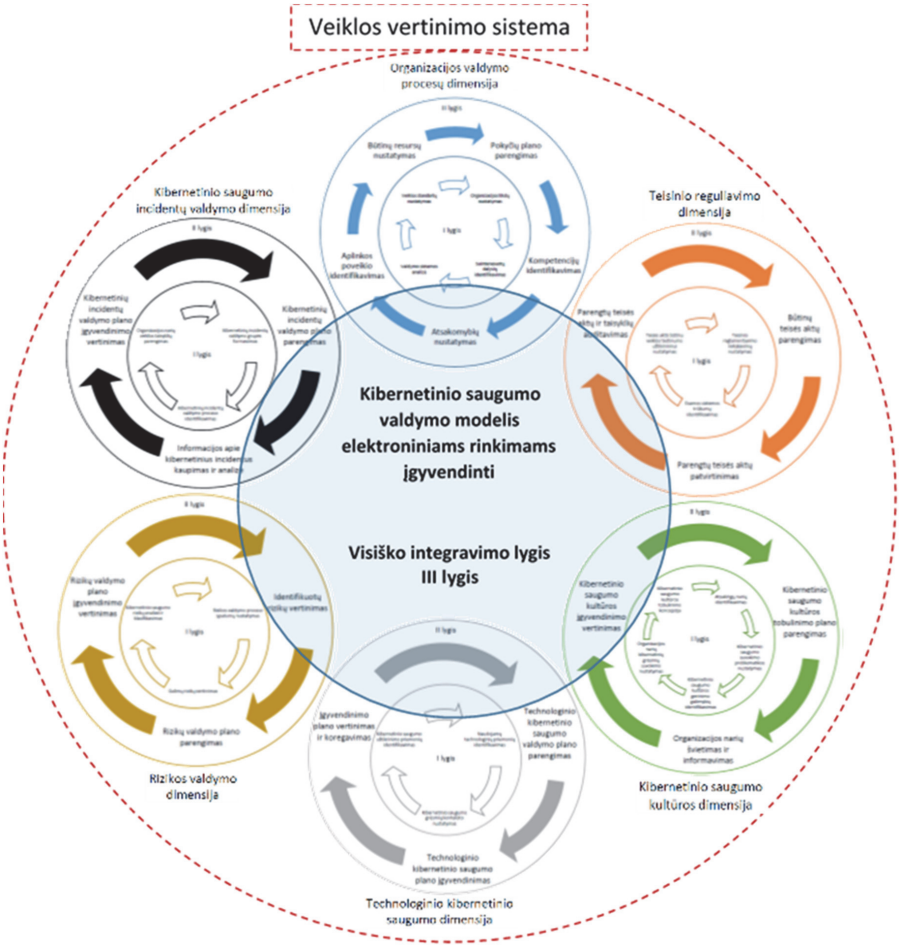
Analizuojamas kibernetinio saugumo valdymo modelis yra technologiškai neutralus, o technologinių priemonių panaudojimas ir kibernetinio saugumo technologinių procesų realizavimas nėra nagrinėjamas šiame disertaciniame darbe.

Nagrinėjant kibernetinio saugumo valdymo modelio struktūrą ir jo pritaikomumą elektroninių rinkimų sistemų įgyvendinimui Lietuvoje, yra pateikiamos tam tikros rekomendacijos, kuriomis galima pasinaudoti, kuriant saugią Lietuvos elektroninių rinkimų sistemą. Modifikuotas konceptualus kibernetinio saugumo valdymo modelis yra pateikiamas 14 paveiksle. Modelio konstravimas buvo vykdomas vadovaujantis disertaciniame darbe anksčiau aptartais T. Parsonso struktūrinio funkcionalizmo principais:

- *tikslo siekimo principas*, numatantis, kad bet kokia sistema turi nusistatyti savo prioritetus ir jų įgyvendinimo eiliškumą;

- *adaptacijos principas*, kuris teigia, kad bet kuri veikianti sistema turi gauti išteklių iš ją supančios aplinkos ir sugebėti juos paskirstyti sistemos viduje;
- *integracijos mechanizmo sukūrimo principas*, numatantis, kad bet kokie sistemoje vykstantis procesai turi būti reguliuojami bei koordinuojami;
- *vertybinių standartų palaikymo principas*, kuris teigia, kad bet kokioje sistemoje turi egzistuoti sistemą sudarančių komponentų valdymo priemonių rinkinys, suderinantis jų veiklą ir tikslus su visos sistemos siekiamais tikslais (Cancian, 1972; VLE, 2012; Voroncov ir kt., 2019).

Detaliai kiekviena patikslinto bei modernizuoto kibernetinio saugumo valdymo modelio elektroniniams rinkimams įgyvendinti dimensija yra išanalizuota sekančiuose disertacijos poskyriuose.



Šaltinis: *Sudaryta autoriaus pagal Limba, Agafonov ir kt., 2017.*

14 paveikslas. *Patikslintas kibernetinio saugumo valdymo modelis e-rinkimams įgyvendinti*

3.2.1. Kibernetinio saugumo valdymo modelio lygių analizė

Atsižvelgiant į kibernetinio saugumo valdymo modelio empirinio tyrimo metu gautus rezultatus ir apibendrinus kibernetinio saugumo ekspertų nuomones, galima teigti, kad kibernetinio saugumo valdymo modelio įgyvendinimą organizacijoje yra tikslinga vykdyti etapais. Visiškai suprantama, kad kuriamo konceptualaus kibernetinio saugumo valdymo modelio įgyvendinimas organizacijoje neabejotinai yra sunkus ir daug resursų reikalaujantis procesas. Siekiant supaprastinti šio kibernetinio saugumo valdymo modelio įdiegimą organizacijoje, yra numatomas modelio dimensijų įgyvendinimas pakopomis, išskiriant tris kibernetinio saugumo valdymo modelio lygius (pakopas): *pradinį (I lygis), vidutinį (II lygis) ir integruotąjį (III lygis*).

Pradinio ir vidutinio lygių diegimo etapuose kiekviena kibernetinio saugumo valdymo modelio dimensija gali būti įgyvendinama, neatsižvelgiant į kitas dimensijas. Vėliau, visoms kibernetinio saugumo valdymo modelio dimensijoms organizacijoje pasiekus antrąjį lygį, organizacija pereina į trečiąjį kibernetinio saugumo valdymo modelio įgyvendinimo etapą – integruotojo organizacijos kibernetinio saugumo valdymo modelio įgyvendinimą, kuomet kiekvienos dimensijos svyravimas iš tam tikros stabilios būsenos automatiškai sukelia kitų dimensijų pokyčius (visos integracijos kibernetinio saugumo valdymo modelio lygis).

Pažymėtina, kad visų siūlomo konceptualaus kibernetinio saugumo valdymo modelio dimensijų pirmasis (pradinis) lygmuo yra siejamas su organizacijos gebėjimais aiškiai nustatyti, kokie kibernetinio saugumo iššūkiai ir problemos egzistuoja organizacijoje. Antrojo kibernetinio saugumo valdymo modelio pakopa yra orientuota į konkrečių organizacijos pokyčiams būtinų veiksmų planų įgyvendinimą, kurie suteikia organizacijai galimybę pagerinti savo kibernetinį saugumą kiekvienos dimensijos ribose. Trečioji pakopa yra skirta kibernetinio saugumo valdymo modeliui harmonizuoti ir visų dimensijų tarpusavyje integruoti, siekiant užtikrinti visapusišką kibernetinį saugumą ir jo valdymą organizacijoje.

Kaip jau buvo minėta anksčiau, pradinis ir vidutinis kibernetinio saugumo valdymo lygiai gali būti diegiami atskiruose kibernetinio saugumo valdymo modelio dimensijose nepriklausomai, tačiau, tik visoms dimensijoms pasiekus antrąjį lygmenį, atsiranda galimybė pereiti į integruotąjį kibernetinio saugumo lygį, kuriame kiekvienos dimensijos pokytis iššaukia kitų dimensijų svyravimus. Kibernetinio saugumo valdymo modelio dimensijų uždaviniai tam tikruose lygiuose yra pateikiami toliau.

Pradinis kibernetinio saugumo valdymo modelio įgyvendinimo lygmuo yra susijęs su organizacijų gebėjimu aiškiai nustatyti, kokie kibernetinio saugumo iššūkiai ir problemos gali būti identifikuojami, įgyvendinant kibernetinį saugumą organizacijoje:

- *Organizacijos valdymo procesai.* Ši dimensija apima organizacijos valdymo sistemos analizę bei suteikia galimybę nustatyti, kuris organizacijos struktūrinis padalinys ar organizacijos narys dalyvauja sprendimų priėmimo procesuose, o šio lygmens pagrindinis uždavinys siejamas su galimybe suteikti organizacijai supratimą, kokie subjektai dalyvauja kibernetinio saugumo valdymo procese ir kokią įtaką kibernetinio saugumo valdymui organizacijoje jie turi;
- *Teisinis reguliavimas*. Šiame lygmenyje kibernetinio saugumo valdymo modelio teisinio reguliavimo dimensijoje yra vykdoma teisinės sistemos analizė

organizacijos viduje ir už jos ribų, taip pat identifikuojami visų teisinių aspektų, galinčių turėti įtakos organizacijos kibernetinio saugumo politikai, reikalavimai ir esami trūkumai;

- *Kibernetinio saugumo kultūra*. Pradiniame šios dimensijos lygmenyje organizacijai iškeliamas tikslas – identifikuoti ir aiškiai suprasti organizacijos naudojamas kibernetinio saugumo priemones, kurios organizacijos viduje gali būti naudojamos, siekiant padidinti kibernetinį saugumą;
- *Technologinis kibernetinis saugumas*. Ši dimensija apima aiškią visų organizacijoje naudojamų technologijų, naudojamų kasdieninio darbo procesui organizuoti, viziją. Tik aiškus požiūris į esamas (egzistuojančias) technologijas, kurios naudojamos organizaciniame gyvenime ir valdymo procesuose, gali nustatyti, kokios kibernetinės atakos gali būti panaudojamos prieš organizaciją, kokie yra galimi technologinių kibernetinių atakų vektoriai ir kokias priemones galima panaudoti atakų prevencijai ar atakų padariniams minimizuoti;
- *Rizikos valdymas*. Pradinio lygmens rizikos valdymo dimensija apibūdina visus rizikos veiksnius ir faktorius, kurie gali atsirasti organizacijoje arba už jos ribų ir gali turėti įtakos organizacijų įprastam gyvenimui ir veikimui;
- *Kibernetinių incidentų valdymas*. Pradiniame lygmenyje šioje dimensijoje organizacija turi įgyti gebėjimą suprasti, kad ji gali būti pažeidžiama technologiniais ar socialiniais aspektais, o pažeidžiamumo, atsirandančio bet kuriuo metu iš bet kokio infrastruktūros segmento (aparatinės ar programinės įrangos) ar personalo, išnaudojimas gali sukelti žalą. Kibernetinių incidentų valdymas šiame lygmenyje gali būti realizuojamas, pasinaudojant parengtomis paprastomis organizacijos veiklos instrukcijomis, kurios gali padėti identifikuoti ir aptikti neįprastą veiklą, nukreiptą prieš organizaciją. Organizacijos ir jos narių supratimas apie kibernetinio saugumo incidentus, jų egzistavimą ir veikimo mechanizmus yra pirmasis, o gal ir pagrindinis žingsnis, siekiant padidinti kibernetinį saugumą organizacijoje.

Apibendrinant pradinį kibernetinio saugumo valdymo modelio lygį, galima teigti, kad šis lygis yra skirtas kibernetinėms grėsmėms ir galimiems pažeidžiamumams organizacijoje identifikuoti bei visų valdymo veiksmų ir atsakomybių paskirstymui organizacijoje nustatyti. Organizacija, įgyvendindama kibernetinio saugumo valdymą, privalo: nustatyti sprendimų, susijusių su organizacijos kibernetiniu saugumu, priėmimo valdymo procesų narius ir jų atsakomybių ribas; išnagrinėti ir nustatyti teisinio reguliavimo pagrindus; įvertinti žmogiškųjų išteklių įtaką kibernetiniam saugumui; nustatyti naudojamas technologijas ir technologinius kibernetinių pažeidžiamumų šaltinius; identifikuoti galimas kibernetinių incidentų atsiradimo rizikas; parengti organizacijos incidentų aptikimo ir informavimo apie juos taisyklių gaires.

Vidutinis kibernetinio saugumo valdymo modelio organizacijoje lygmuo numato kiekvienos iš šešių kibernetinio saugumo valdymo modelio dimensijų išsivystymą, nustatant aiškų pokyčių valdymo planą ir pateikiant organizacijai būtinų atlikti veiksmų sąrašą:

- *Organizacijos valdymo procesai*. Turi būti aiškiai apibrėžiama valdymo grandinė, sureguliuoti organizacijos sprendimų priėmimo procesai, nustatytos aiškios organizacijos narių atsakomybės ribos;

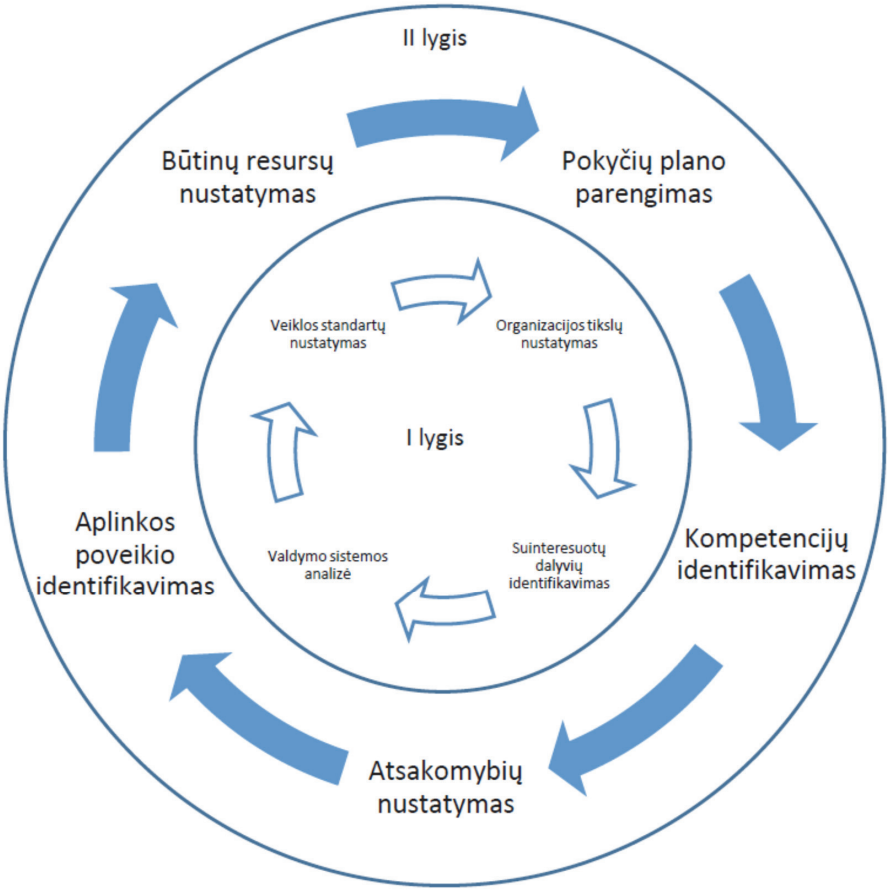
- *Teisinis reguliavimas*. Turi būti aiškiai įvardyti teisiniai organizacijos veiklos aspektai, kiekvienam organizacijos nariui turi būti parengtos ir pateiktos visos veiklos instrukcijos ir taisyklės, taip pat turi būti vykdomas periodinis teisinio reglamentavimo sistemos auditas;
- *Kibernetinio saugumo kultūra*. Šiame išsivystymo lygmenyje kibernetinio saugumo modelio dimensijoje yra nagrinėjamas personalo valdymas, identifikuojami būtini personalo įgūdžiai, numatomi organizacijos narių mokymai, kadangi visi organizacijos nariai prisideda prie organizacijos kibernetinio saugumo, o tik kvalifikuotas informacinių technologijų aptarnavimo personalas neturėtų būti kibernetinio saugumo užtikrinimo garantija organizacijoje;
- *Technologinis kibernetinis saugumas*. Technologijų valdymas turi aiškiai ir suprantamai identifikuoti organizacijos naudojamą techninę ir programinę įrangą, įskaitant naudojamos įrangos gyvavimo ciklą, nes didžiausia dalis kibernetinio saugumo pažeidimų yra paslėpta būtent technologinėse sistemose, kurios yra pasenusios, tačiau vis dar naudojamos organizacijų veiklos procesuose. Technologinis auditas turi būti atliekamas nuolat, nes tik jis leis organizacijai tinkamai planuoti ateities finansinius išteklius, reikalingus technologinėms sistemoms atnaujinti ir palaikyti;
- *Rizikos valdymas*. Šiame kibernetinio saugumo valdymo modelio lygyje rizikos valdymo dimensija sukonkretizuoja kibernetinio saugumo valdymo rizikas, nustatytas pradiniame lygmenyje, bei apibrėžia aiškius šių rizikų valdymo planus;
- *Kibernetinių incidentų valdymas*. Šiame valdymo modelio lygmenyje incidentų valdymo dimensija nagrinėja organizacijos pasirengimą galimiems kibernetinio saugumo incidentams. Organizacija ir jos nariai turi būti parengę išsamius kibernetinių incidentų valdymo ir organizacijos veiklos atkūrimo planus, o kiekvienas organizacijos narys ar skyrius turi žinoti atkūrimo planą ir savo veiksmus, kaip atstatyti organizacijos kasdienę veiklą po įvykusio ar vykstančio kibernetinio saugumo incidento.

Apibendrinant vidutinį kibernetinio saugumo valdymo modelio lygį organizacijoje, galima teigti, kad šis lygis yra siejamas su organizacijos gebėjimu vykdyti kibernetinių incidentų ir grėsmių nustatymą, bei organizacijos pasiruošimu valdyti šios incidentus visuose kibernetinio saugumo valdymo modelio dimensijose. Įgyvendindama šį lygį, organizacija turi aiškiai nustatyti organizacijos narių atsakomybės ribas ir valdymo grandinę; parengti teisinio reguliavimo dokumentus, reglamentuojančius aiškias kibernetinio saugumo valdymo organizacijoje nuostatas; parengti personalo švietimo ir tobulinimo koncepcijas; parengti technologijų valdymo planą; atlikti rizikos vertinimą ir valdymą; parengti kibernetinių incidentų išvengimo ir įvykusių incidentų padarinių šalinimo planus.

Aukščiausias kibernetinio saugumo valdymo modelio lygis pasiekiamas organizacijoje yra *visiškos integracijos (sąveikos) lygis*, kuris nustato visą kibernetinio saugumo valdymo modelio dimensijų tarpusavio integravimą ir veikimą. Šiame lygyje organizacija ir jos nariai veikia kaip viena didelė ekosistema, o kiekviena kibernetinio saugumo valdymo modelio dimensija tampa neatskiriama organizacijos veiklos tęstinumo proceso dalimi.

3.2.2. Organizacijos valdymo procesų dimensijos analizė

Organizacijos valdymo procesų dimensija kibernetinio saugumo valdymo modelio kontekste yra svarbiausia organizacijos kibernetinio saugumo valdymo modelio dalis. Būtent ši dimensija užtikrina sėkmingą tolimesnį kibernetinio saugumo valdymo modelio panaudojimo ir sėkmingo pritaikymo organizacijoje galimybę. Organizacijos valdymo procesų dimensija grafiškai yra pavaizduojama žemiau esančiame paveiksle (žr. 15 paveikslą).



Šaltinis: *Sudaryta autoriaus*

15 paveikslas. *Organizacijos valdymo procesų dimensija*

Kaip jau buvo minėta anksčiau, šiame disertaciniame darbe, nagrinėjant kibernetinio saugumo valdymą elektroninių rinkimų sistemų kontekste, valstybė yra traktuojama kaip organizacija, kadangi rinkimų ir referendumų organizavimas, vykdymas ir rinkimų saugumo užtikrinimas yra išskirtinė valstybės prerogatyva, įgyvendinama per

tam tikrus įgaliotus subjektus. Vyriausioji rinkimų komisija (toliau – VRK) yra *Lietuvos Respublikos Konstitucijoje numatyta nuolatinė aukščiausioji rinkimų ir referendumų organizavimo bei vykdymo valstybės institucija, kuri įstatymų nustatyta tvarka vykdo ir organizuoja Seimo, Prezidento ir savivaldybių tarybų rinkimus, taip pat referendumus* (VRK, 2018), o Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC) turi būti *pagrindinė Lietuvos kibernetinio saugumo institucija, atsakinga už vieningą kibernetinių incidentų valdymą, kibernetinio saugumo reikalavimų įgyvendinimo stebėseną ir kontrolę* (NKSC, 2018), diegiant ir eksploatuojant elektroninių rinkimų sistemas.

Pažymėtina, kad kibernetinio saugumo modelio organizacijos valdymo procesų dimensija yra susieta su tokiomis svarbiomis organizacijos valdymo sritimis, kaip organizacijos strateginis valdymas, vadovavimas, standartų taikymas organizacijos veikloje bei veiklos efektyvumo vertinimo sistema, kadangi būtent šios sritys yra labai svarbios, kuriant naują arba transformuojant egzistuojančią organizaciją, o kiekvienos organizacijos vadovas privalo galvoti apie strategiją, valdymą ir standartus, taikomus visose organizacijos veiklos srityse, siekdamas suderinamumo ir balanso tarp kibernetinio saugumo ir rizikos priimtinumo, tarp naudojamų technologijų ir verslo tikslų, tarp galimos rizikos ir siekiamos naudos (Kaplan, Norton, 2001; Moschovitis, 2018).

Toliau esančioje lentelėje yra pateikiamas kibernetinio saugumo valdymo modelio organizacijos valdymo procesų dimensijos organizacinės struktūros priemonių detalizavimas (žr. 9 lentelę).

9 lentelė. *Organizacijos valdymo procesų dimensijos įgyvendinimo priemonės*

<table>
<tr><th colspan="3">Organizacijos valdymo procesų dimensija</th></tr>
<tr><th>1 lygis</th><th>2 lygis</th><th>3 lygis</th></tr>
<tr><td>Organizacijos tikslų nustatymas.</td><td>Organizacijos veiklos pokyčių plano parengimas:
sprendimo priėmimo proceso modelio identifikavimas;
numatytų tikslų įgyvendinimo priemonės ir užduotys organizacijos nariams;
funkcinių veiklos sričių paskirstymas.</td><td rowspan="6">Organizacijos valdymo procesų dimensijos integravimas ir sujungimas su kitomis kibernetinio saugumo valdymo modelio dimensijomis.</td></tr>
<tr><td>Suinteresuotų dalyvių identifikavimas.</td><td>Organizacijos ir jos narių būtinų kompetencijų nustatymas.</td></tr>
<tr><td>Organizacijos valdymo sistemos ir sprendimų priėmimo proceso identifikavimas.</td><td>Organizacijos narių atsakomybės ribų identifikavimas.</td></tr>
<tr><td rowspan="2">Organizacijos veiklos standartų nustatymas.</td><td>Organizacijos aplinkos identifikavimas.</td></tr>
<tr><td>Resursų ir pajėgumų identifikavimas.</td></tr>
</table>

Šaltinis: *Sudaryta autoriaus*

Organizacijos valdymo procesų dimensijos pirmame lygyje organizacija turi įgyvendinti toliau išvardytas priemones:

- *Nusistatyti tikslus*. Šio etapo metu organizacija privalo identifikuoti ir apibrėžti ilgalaikius ir trumpalaikius jos siektinus tikslus bei detalizuoti šių tikslų įgyvendinimo procesą, suskirstant jį į tam tikrus etapus, kurių įgyvendinimas laiku ir nuosekliai suteiktų organizacijai galimybę pasiekti užsibrėžtą ilgalaikį tikslą. Elektroninių rinkimų įgyvendinimo kontekste pagrindinis ilgalaikis valstybės tikslas, be jokios abejonės, yra siejamas su saugių ir patikimų elektroninių rinkimų įgyvendinimu šalyje, o trumpalaikiai valstybės siekiami tikslai gali būti tapatinami su tam tikrų elektroninių rinkimų rūšių įgyvendinimu (pvz., rinkimų, panaudojant elektroninius balsavimo įrenginius rinkimų apylinkėse, įgyvendinimas; internetinių rinkimų įgyvendinimas; elektroninių rinkimų sistemų, naudojančių išmaniuosius įrenginius balsavimo procese, įdiegimas);
- *Identifikuoti suinteresuotus dalyvius*. Šiame etape turi būti identifikuojamos visos šalys (*angl. stakeholder*), kurios vienaip ar kitaip dalyvauja organizacijos vykdomuose procesuose, daro įtaką šiems procesams arba yra priklausomi nuo organizacijos vykdomos veiklos. Šiame etape turi būti atliekamas ne tik jau žinomų suinteresuotų šalių nustatymas, bet ir identifikuojami visi asmenys, kurie vienaip ar kitaip gali veikti organizaciją arba būti veikiami organizacijos. Elektroninių rinkimų kontekste galima sakyti, kad į suinteresuotųjų grupę gali patekti: valstybės piliečiai, visuomeninės organizacijos, techninės ir programinės įrangos tiekėjai, duomenų perdavimo sistemų operatoriai, kibernetinio saugumo sprendimus ir technologijas parduodančios kompanijos, organizacijos, atsakingos už valstybės kibernetinio saugumo politikos formavimą, įgyvendinimą ir priežiūrą, bei organizacijos atsakingos už rinkimų organizavimą, vykdymą ir kontrolę;
- *Identifikuoti valdymo sistemą ir sprendimų priėmimo procesą*. Sprendimo priėmimo proceso dalyvių ir jų įtakos sprendimo priėmimui nustatymas leis organizacijai užtikrinti esamos sistemos modernizavimą bei, esant būtinumui, atlikti šios sistemos korekcijas;
- *Nustatyti organizacijos veiklos standartus*. Šiame etape pirmiausia nustatoma, ar dabartinis organizacijos veiklos ir valdymo modelis, vidinių procesų organizavimas, personalo valdymas, rizikos valdymas ir kitos sritys yra tvarkomos, pasinaudojant egzistuojančiomis ir pasaulyje pripažintomis gerosiomis praktikomis ir standartais. Atlikus organizacijos naudojamų konkrečių standartų ir praktikų auditą bei įvertinus organizacijos veiklos sritį, galima aiškiai identifikuoti, kokie papildomi standartai turi būti įdiegti ateityje. Taip pat šiame etape yra būtina atlikti ir suinteresuotų dalyvių (dalyvaujančių organizacijos veikloje įrangos tiekėjų, ryšio operatorių ir kt.) taikomų standartų analizę, kadangi organizacija, siekianti tam tikrų standartų, pvz., kibernetinio saugumo srityje, turi naudoti patikimą kitų gamintojų ar tiekėjų techninę ir programinę įrangą. Diegiant elektroninių balsavimų sistemas, yra būtinas technologinės įrangos naudojimas, bet ne visa technologinė įranga yra patikima (Salinas, 2018), o nepatikimos techninės įrangos panaudojimas, organizuojant elektroninius balsavimus, gali sužlugdyti visuomenės pasitikėjimą sistema.

Organizacijai įgyvendinus kibernetinio saugumo valdymo modelio organizacijos valdymo procesų dimensijos pirmojo lygio priemones, gali būti toliau žengiama prie šios dimensijos įgyvendinimo tobulinimo (antrojo lygio) ir pradedamos įgyvendinti toliau išvardytos priemonės:

- *Organizacijos veiklos pokyčių plano parengimas*, kuris turi aiškiai nusakyti ir apibrėžti būsimą organizacijos sprendimo priėmimo proceso modelį (sprendimo priėmimo proceso dalyvius, jų įgaliojimus, funkcijas, veiklos apribojimus ir kt.); organizacijos numatytų ilgalaikių ir trumpalaikių tikslų įgyvendinimo priemones ir užduotis organizacijos nariams, įgyvendinantiems ar prisidedantiems prie konkrečių tikslų įgyvendinimo; konkrečių organizacijos narių kuruojamų sričių paskirstymą, narių dalyvavimą konkrečiuose organizacijos veiklos procesuose, atliekamas rutinines užduotis. Lietuvos elektroninių rinkimų proceso įgyvendinimo kontekste šios priemonės įgyvendinimo procese privalo dalyvauti VRK, Lietuvos Respublikos krašto apsaugos ministerija (toliau – KAM), NKSC, Lietuvos Respublikos teisingumo ministerija (toliau – TM), Lietuvos Respublikos valstybės saugumo departamentas (toliau – VSD), Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos (toliau – AOTD), Lietuvos Respublikos vidaus reikalų ministerija (toliau – VRM). Taip pat pažymėtina, kad papildomai gali būti svarstomas privataus sektoriaus (verslo įmonių, įgyvendinančių kibernetinio saugumo sprendimus) pajėgumų, akademinės visuomenės ir kitų suinteresuotų subjektų įtraukimas į šios priemonės įgyvendinimo procesą;
- *Organizacijos ir jos narių būtinų kompetencijų identifikavimas*. Šios priemonės įgyvendinimo metu būtina nustatyti organizacijos nariams keliamus minimalius reikalavimus (būtinas kompetencijas). Visų organizacijos narių atitikimas keliamiems reikalavimams užtikrins sėkmingą ir kokybišką organizacijos vykdomų funkcijų ir veiklos procesų įgyvendinimą. Nagrinėjant šią priemonę elektroninių rinkimų įgyvendinimo kontekste, galima teigti, kad organizacijos nariai privalo turėti šias kompetencijas: rinkimų organizavimas, vykdymas ir stebėjimas; kibernetinio saugumo užtikrinimas. Būtina pažymėti, kad Lietuvos atveju už rinkimų organizavimą, vykdymą ir stebėjimą yra (ir tikėtina, kad bus) atsakinga VRK, o už kibernetinio saugumo įgyvendinimą, užtikrinimą, stebėjimą ir palaikymą gali būti atsakingi kiti subjektai, paskirstant jų atsakomybės ribas, atsižvelgiant į jiems suteiktų įgaliojimų ir vykdomos veiklos ypatumus;
- *Organizacijos narių atsakomybės ribų identifikavimas*, nurodantis, už kokius organizacijoje vykstančius procesus (šių procesų tarpinius rezultatus) yra atsakingas kiekvienas organizacijos narys. Įgyvendinant šią priemonę, turi būti aiškiai ir tiksliai nurodyta kiekvieno organizacijos nario atsakomybė, vykdant tam tikrą organizacijos veikos proceso dalį;
- *Aplinkos identifikavimas*, galintis vienareikšmiškai apibrėžti vidaus ir išorės aplinkas bei šių aplinkų poveikį organizacijos vykdomiems ir ateityje planuojamiems vykdyti veiklos procesams. Įgyvendinant šią priemonę, reikia įvertinti organizacijos naudojamas technologines priemones, vykdomas užduotis ir

procesus, personalą ir jo santykius, organizacijos hierarchinę struktūrą, taip pat geopolitinę, sociokultūrinę, ekonominę ir technologinę aplinkas, kuriuose egzistuoja organizacija, kadangi būtent šie organizacijos aplinkos aspektai daro įtaką būsimiems (ir vykstantiems) organizacijos pokyčiams ir resursų bei pajėgumų poreikiams, būtinus organizacijos transformacijos procesui įgyvendinti;

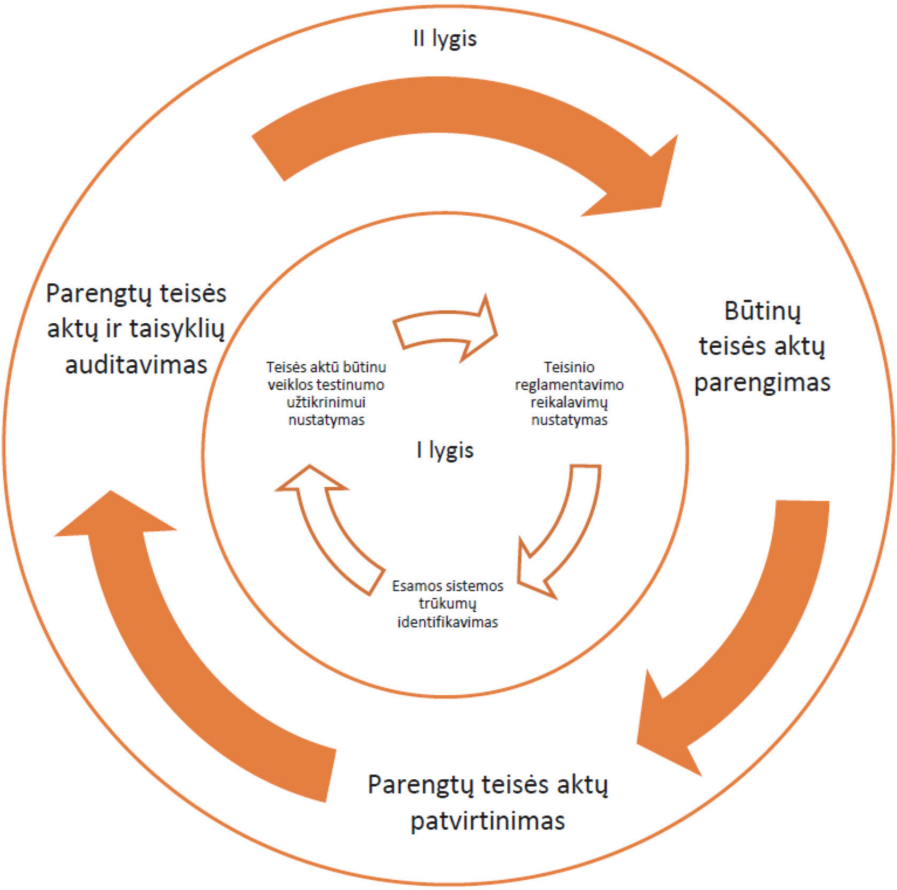
- *Resursų ir pajėgumų identifikavimas* yra būtinas, siekiant nustatyti priemones, kurios naudojamos (arba bus panaudotos ateityje) organizacijos veikloje, siekiant užtikrinti vykdomų veiklos procesų tęstinumą. Šiame etape organizacija turi aiškiai identifikuoti, apibrėžti bei detalizuoti visus organizacijos veikloje panaudojamus išteklius. Šis procesas leis efektyviai paskirstyti materialines ir nematerialines priemones bei sudaryti išteklių paskirstymo ir panaudojimo planus, kurie suteiks galimybę tinkamai ir efektyviai įgyvendinti nustatytus tikslus.

Kaip jau buvo minėta anksčiau, įgyvendinant kibernetinio saugumo valdymo modelį organizacijoje, kiekviena modelio dimensija gali būti įgyvendinama atskirai, t. y. nustatant dabartinę kiekvienos kibernetinio saugumo dimensijos būklę, identifikuojant siektinus tikslus bei sudarant organizacijos veiklos procesų pokyčių planą, kuriame atsispindėtų tikslų pasiekimo etapai. Toks dimensijų įgyvendinimas įmanomas iki tol, kol kiekviena modelio dimensija pasieks antrąjį lygį. Tuomet kibernetinio saugumo valdymo modelio įgyvendinimas pereina į trečiąjį lygmenį, kuriame visos dimensijos tampa priklausomos viena nuo kitos, o pati organizacija veikia kaip viena didelė ekosistema, kurios komponentai veikia vienas kitą. Požiūris į organizaciją kaip į ekosistemą užtikrina kibernetinio saugumo kompleksiškumą bei suteikia organizacijai galimybę efektyviai priešintis išorinėms ir vidinėms kibernetinėms grėsmėms, taip pat efektyviai reaguoti į kibernetinius incidentus.

Pažymėtina, kad, įgyvendinant kibernetinio saugumo valdymo dimensija organizacijoje, yra būtina atlikti ir įgyvendinimo proceso stebėjimą bei vertinimą. Šiam tikslui pasiekti organizacija turi sukurti ir naudoti veiklos efektyvumo vertinimo sistemą. Šios sistemos funkcijos ir organizacijos veiksmai, planuojant ir įgyvendinant veiklos efektyvumo vertinimo sistemą, bus pateikti vėliau.

3.2.3. Teisinio reguliavimo dimensijos analizė

Šiame disertaciniame darbe kibernetinio saugumo valdymo modelio teisinio reglamentavimo dimensija yra nagrinėjama tik iš įstatyminio teisinio reguliavimo perspektyvos, suteikiančios organizacijai, vykdančiai elektroninius rinkimus, tam tikrus, įstatymo numatytus, įgaliojimus, atliekant elektroninio balsavimo organizavimo, vykdymo ir kontrolės funkcijas. Disertaciniame darbe nebus nagrinėjami klausimai, susiję su kibernetinio saugumo incidentų sukėlėjų teisinio persekiojimo problematika, teisinio persekiojimo jurisdikcijos problemomis bei teisės aktais, reglamentuojančiais valstybių piliečių elgesį elektroninėje erdvėje, nors šios problemos šiuolaikiniame pasaulyje, kuriame beveik kiekvienoje visuomenės veiklos srityje yra panaudojamos informacinės ir telekomunikacinės technologijos, yra labai aktualios (Appazov, 2014). Kibernetinio saugumo valdymo modelio teisinio reguliavimo dimensija grafiškai yra pavaizduojama žemiau esančiame paveiksle (žr. 16 paveikslą).



Šaltinis: *Sudaryta autoriaus*

16 paveikslas. *Teisinio reguliavimo dimensija*

Kuriamo kibernetinio saugumo valdymo modelio teisinio reguliavimo dimensija yra susijusi su kibernetinio saugumo valdymo teisiniu įgyvendinimu, kuris apima organizacijos vykdomos veiklos teisinį reguliavimą, organizacijos atitikimą teisės normoms ir keliamiems reikalavimams, siekiant sklandžiai įgyvendinti kibernetinio saugumo valdymą organizacijos veikloje. Pažymėtina, kad šios kibernetinio saugumo valdymo modelio dimensijos įgyvendinimas gali būti skirstomas į dvi stambias sritis:

1. *Organizacijos išorinės* aplinkos teisinis reguliavimas, kuris yra susijęs su nacionalinių, Europos Sąjungos ir kitų organizacijų teisės aktais, reglamentuojančiais bei formuojančiais organizacijos veiklą kibernetinio saugumo įgyvendinimo srityje. Pasaulio mokslininkai pažymi, kad išorinės aplinkos įtaka organizacijai nepriklauso nuo pačios organizacijos ir jos vykdomos veiklos, o organizacijai įtaką

darantys veiksniai yra kuriami (sudaromi) už organizacijos ribų, tačiau, organizacija gali (o dažniausiai privalo) imtis tam tikrų priemonių, siekdama pakeisti susidariusią (dažniausiai organizacijai nepalankią) situaciją ir prisitaikyti prie besikeičiančios aplinkos sąlygų (Kefalas, 1987; Sakalas, 2003; Zakarevičius ir kt., 2004);

2. *Organizacijos vidinės aplinkos teisinis reguliavimas*, nusakantis organizacijos vidaus teisinio reglamentavimo ir tvarkos taisyklių įgyvendinimą. Ši sritis yra siejama su organizacijos siekiu tobulinti vidaus administravimo teisinių priemonių įgyvendinimą, organizacijos narių vykdomų funkcijų ir atsakomybės ribas reglamentuojančių teisės aktų parengimu ir kt.

Pažymėtina, kad abi anksčiau minėtos teisinio reguliavimo sritys yra vienodai svarbios sėkmingam kibernetinio saugumo valdymo proceso įgyvendinimui organizacijoje, taip pat ir tolimesniam organizacijos vystymuisi bei jos vykdomų veiklos procesų tęstinumui užtikrinti. Abi šios sritys yra glaudžiai susijusios tarpusavyje, kadangi išorinės aplinkos pokyčiai dažniausiai sąlygoja organizacijos vidaus aplinkos pokyčių atsiradimą. Organizaciją veikianti išorinė aplinka yra labai dinamiška, priklausanti nuo daugelio faktorių, todėl organizacija privalo ją nuolat stebėti, prognozuoti galimus pokyčius bei būti pasirengusi prie jų prisitaikyti. Išorinėje aplinkoje atsirandantys pokyčiai neabejotinai paveiks ir organizacijos vidaus aplinką, tačiau, vykdant išorinės aplinkos stebėjimą ir pasirengus ateities pokyčiams, šios aplinkos pakeitimai organizacijai nebus netikėti.

Siūlomo kibernetinio saugumo valdymo modelio kontekste teisinio reglamentavimo dimensijos sritys nebus nagrinėjamos atskirai, kadangi organizacijos ir jos narių veiksmai, įgyvendinant kibernetinį saugumą organizacijoje, yra susieti tiek su išorinės, tiek su vidinės aplinkos pokyčiais, o kaip buvo pažymėta anksčiau, organizacija gali iš dalies veikti išorinės aplinkos pokyčius bei visiškai valdyti vidinės aplinkos pokyčius.

Toliau esančioje lentelėje yra pateiktas kibernetinio saugumo valdymo modelio teisinio reglamentavimo dimensijos organizacinės struktūros priemonių detalizavimas (žr. 10 lentelę).

10 lentelė. *Teisinio reglamentavimo dimensijos įgyvendinimo priemonės*

<table>
<tr><th colspan="3">Teisinio reglamentavimo dimensija</th></tr>
<tr><th>1 lygis</th><th>2 lygis</th><th>3 lygis</th></tr>
<tr><td>Organizacijos teisinio reglamentavimo sistemos analizė:
esamos teisinio reglamentavimo sistemos reikalavimų nustatymas;
esamos teisinio reglamentavimo sistemos trūkumų identifikavimas.</td><td>Teisės aktų ir taisyklių, būtinų organizacijos veiklos procesų tęstinumui užtikrinti, parengimas ir patvirtinimas.</td><td rowspan="2">Teisinio reglamentavimo dimensijos integravimas ir sujungimas su kitomis kibernetinio saugumo valdymo modelio dimensijomis.</td></tr>
<tr><td>Teisės aktų ir taisyklių, būtinų organizacijos veiklos procesų tęstinumui užtikrinti, identifikavimas.</td><td>Parengtų teisės aktų ir taisyklių taikymo bei naudojimo organizacijoje auditas.</td></tr>
</table>

Šaltinis: *Sudaryta autoriaus*

Teisinio reglamentavimo dimensijos pirmame lygyje organizacija turi įgyvendinti toliau išvardytas priemones:

- *Organizacijos teisinio reglamentavimo sistemos analizės* priemonę, suteikiančią organizacijai galimybes nustatyti organizacijai taikomo teisinio reguliavimo reikalavimus bei organizacijos veiklą reglamentuojančių teisės aktų trūkumus. Nagrinėjant šią priemonę Lietuvos elektroninių rinkimų kontekste, galima teigti, kad yra būtina išnagrinėti dabartinę rinkimų sistemą ir valstybės kibernetinį saugumą reglamentuojančius teisės aktus: rinkimų įstatymus; VRK nuostatus ir jai pavestų vykdyti funkcijų teisinį reglamentavimą; valstybės kibernetinį saugumą reglamentuojančius teisės aktus; NKSC veiklos nuostatus ir vykdomas funkcijas; valstybės ypatingos svarbos infrastruktūros naudojimą reglamentuojančius dokumentus; kitų organizacijos narių, dalyvaujančių ar dalyvausiančių elektroninių rinkimų procese, taip pat atsakingų už valstybės ypatingos svarbos infrastruktūrą bei šioje infrastruktūroje veikiančių informacinių sistemų valdymą ir kontrolę. Pažymėtina, kad, įgyvendinant šią priemonę ir atliekant teisinio reglamentavimo sistemos analizę, organizacija privalo nagrinėti ne tik išorinę organizacijos aplinką, bet didelį dėmesį sutelkti ir į vidinės aplinkos aspektus, kurių analizė suteiks organizacijai žinių apie vidinėje aplinkoje esančias teisinio reglamentavimo spragas;
- *Teisės aktų ir taisyklių, būtinų organizacijos veiklos procesų tęstinumui užtikrinti, identifikavimo* priemonė suteikia organizacijai galimybę identifikuoti, koks teisės aktų ar vidaus tvarkos taisyklių rinkinys yra būtinas, norint užtikrinti sklandų organizacijos vykdomos veiklos ir vykstančių procesų tęstinumą. Šios priemonės įgyvendinimas yra neatsiejamas nuo teisinio reglamentavimo sistemos analizės priemonės, kadangi tik išsamios analizės rezultatai gali suteikti organizacijai pakankamą kiekį duomenų, reikalingų teisinio reguliavimo sistemos spragoms identifikuoti. Įgyvendindama šią priemonę, organizacija turės pakankamai duomenų, reikalingų galimai besidubliuojantiems teisės aktams ar jų nuostatoms identifikuoti, gebės identifikuoti organizacijos narių vykdomas funkcijas bei galės nustatyti šių funkcijų dubliavimąsi organizacijoje. Šios priemonės įgyvendinimo procesas suteiks organizacijai galimybę ne tik patobulinti ir patikslinti teisinį reglamentavimą, peržiūrėti organizacijos vykdomas veiklas ir procesus, patobulinti visos organizacijos strategiją bei jos narių vykdomas funkcijas, bet gali padėti organizacijai identifikuoti netikslingą išteklių panaudojimą bei atskleisti šių išteklių panaudojimo optimizavimo galimybes ir būdus.

Organizacijai įgyvendinus kibernetinio saugumo valdymo modelio teisinio reglamentavimo dimensijos pirmojo lygmens priemones, organizacija gali pradėti įgyvendinti antrajame dimensijos lygyje įvardytas priemones:

- *Teisės aktų ir taisyklių, būtinų organizacijos veiklos procesų tęstinumui užtikrinti, parengimas ir patvirtinimas*. Šios priemonės įgyvendinimas yra susijęs su organizacijos ir jos narių gebėjimais įgyvendinti teisinio reglamentavimo korekcijas, suteikiančias organizacijai galimybę užtikrinti savo vykdomos veiklos ir organizacijos viduje vykstančių procesų tęstinumą. Nagrinėjant šios priemonės

įgyvendinimą organizacijos išorinės aplinkos kontekste, būtina pažymėti, kad organizacija dažniausiai negali daryti įtakos išorinei aplinkai, tačiau privalo stengtis pakeisti šią aplinką. Lietuvos elektroninių rinkimų sistemos įgyvendinimo kontekste vienas iš esminių probleminių teisinio reglamentavimo klausimų yra siejamas su elektroninių rinkimų sistemų įteisinimu ir jų panaudojimu, vykdant rinkimus ir referendumus Lietuvoje. Paskutinį dešimtmetį Lietuvoje ne vieną kartą buvo bandoma įteisinti elektroninius balsavimus, tačiau tai taip ir nebuvo atlikta. Pagrindinė susidariusios situacijos priežastis yra siejama su politinės valios stoka. Taip pat pastebima, kad elektroniniai rinkimai ir jų įteisinimas bei įgyvendinimas Lietuvoje tapo savotišku politikų ir partijų politinio kapitalo didinimo įrankiu, kuris yra naudojamas, siekiant pritraukti kuo didesnį rinkėjų susidomėjimą prieš rinkimus (Limba ir kt., 2017). Tačiau, įvykus rinkimams, pažadai dėl elektroninių rinkimų įgyvendinimo taip ir lieka tik politikų pažadais, o valstybės piliečiams yra suformuojama nuomonė, kad elektroninių rinkimų įgyvendinimas neabejotinai sukels grėsmę valstybės saugumui, nes visiškas technologinis saugumas ir balsavimo slaptumas yra neįmanomi (Jurčenkaitė, 2019). Pažymėtina, kad VSD ir AOTD 2019 metų grėsmių nacionaliniam saugumui vertinime yra pažymėję, kad „Rusija išnaudoja kibernetinę erdvę daryti įtaką Vakarų valstybėse vykstantiems politiniams procesams, siekia paveikti rinkimų rezultatus, sumenkinti visuomenės pasitikėjimą demokratinių procesų ir politinės santvarkos patikimumu“ (VSD, AOTD, 2019), tačiau pateikta nuostata apima ne tiek tradicinius technologinius kibernetinius išpuolius prieš elektronines balsavimo sistemas, apie kurias dažniausiai užsimina Lietuvos politikai (Jurčenkaitė, 2019), bet labiau charakterizuoja Rusijos naudojamus šiuolaikinio hibridinio karo (*angl. hybrid warfare*) metodus, elementus bei technologijas (Barojan, 2018; Krauel, Bay, 2018; NATO StratCom COE, 2018), kuriomis yra bandoma formuoti visuomenės nuomonę apie tam tikrus politinius veikėjus. Tokius veiksmus galima klasifikuoti kaip socialinės inžinerijos priemonėmis atliekamą kibernetinę ataką, kurios metu dažniausiai nėra panaudojamos technologinio poveikio priemonės ir nesiekiama įvykdyti technologinės kibernetinės atakos. Nagrinėjant šios priemonės įgyvendinimą organizacijos vidinės aplinkos kontekste, būtina pažymėti, kad teisinis reguliavimas organizacijoje neturi prieštarauti aukštesnių (norminių) teisės aktų reikalavimams, kurie gali nusakyti, kokie organizacijos teisinio reguliavimo principai turi būti įgyvendinti organizacijos veikloje. Organizacija, atsižvelgdama į savo patirtį, veiklos specifiką, istoriją ir praeities precedentus, gali pasitvirtinti ir papildomą vidaus aplinkos teisinio reguliavimo sistemą, pvz., darbuotojų ir informacinių sistemų administratorių darbo su informacinėmis sistemomis taisykles, interneto ir elektroninio pašto naudojimo taisykles, išorinių laikmenų panaudojimo organizacijos kompiuteriniuose tinkluose taisykles ir kt. Elektroninių rinkimų sistemų įgyvendinimo kontekste vidinės aplinkos teisinis reguliavimas neabejotinai bus susietas su valstybės naudojamų kritinės infrastruktūros informacinių sistemų teisiniu reglamentavimu, Europos Sąjungos Bendrųjų duomenų apsaugos reglamentu ir

kitomis taisyklėmis, Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu ir kitais teisės aktais ir reikalavimais, kurie yra privalomai taikomi, diegiant, administruojant ir naudojant elektroninių rinkimų sistemas;

- *Parengtų teisės aktų ir taisyklių taikymo ir naudojimo organizacijoje auditas*, suteiksiantis organizacijai galimybes išvengti teisinių spragų atsiradimo organizacijos ir jos narių veiklą reglamentuojančiuose teisinio reguliavimo dokumentuose ir taisyklėse. Auditavimo priemonės įgyvendinimas ir naudojimas organizacijoje, taip pat kaip ir kitų šioje dimensijoje esančių priemonių įgyvendinimas organizacijos veiklos procesuose, yra siejamas su vidine ir išorine aplinkomis, t. y. su išorinės ir vidinės aplinkos audito galimybėmis. Auditavimo priemonių įgyvendinimas išorinės aplinkos kontekste turi būti siejamas su išoriniu organizacijos auditu, siekiant identifikuoti valstybės (taip pat ir tarptautinio) lygmens reglamentuojančių teisinių normų, poįstatyminių teisės aktų trūkumus ar būtinus atlikti teisės aktų pakeitimus. Išorinės aplinkos auditas dažniausiai atliekamas, pasinaudojant audito paslaugas teikiančių kompanijų paslaugomis, kurias perka pati organizacija. Taip pat gali būti vykdomas ir valstybės auditas, siekiant nustatyti tam tikrų teisinio reguliavimo normų ar poįstatyminių teisės aktų įgyvendinimą organizacijos veikloje. Vidinės aplinkos auditas dažniausiai vykdomas po išorinės aplinkos auditavimo, tačiau pati organizacija privalo suprasti, kad vidaus auditas yra organizacijai būtinas periodinis procesas, kuris turi būti vykdomas, siekiant laiku identifikuoti vidinių taisyklių ir reglamentuojančių teisės aktų neatitikimą realiems organizacijos veiklos procesams, tokiu būdu suteikiant organizacijai galimybę atitikti išorinio teisinio reglamentavimo keliamus reikalavimus. Vidinės aplinkos auditavimą dažniausiai vykdo tam tikras organizacijos padalinys, kuris yra nepriklausomas nuo kitų organizacijos skyrių, o už savo įvykdytą veiklą atsiskaito aukščiausiai organizacijos vadovybei. Kitaip tariant, organizacijos vidaus auditas gali būti apibūdinamas kaip tam tikra organizacijoje atliekama funkcija (biurokratinė veikla), kurią vykdo gerai apmokyti specialistai (profesionalai), turintys autonomiją savo darbui atlikti (Jones, 2013). Autonomiškumas ir išskirtinis pavaldumas aukščiausiajai organizacijos vadovavimo ir valdymo teises turinčiai grandžiai suteikia vidaus audito funkciją vykdančiam padaliniui visišką veiklos laisvę bei įgalina jį visapusiškai ir nešališkai vertinti organizacijoje vykstančius veiklos procesus ir visos organizacijos ar atskirų jos narių vykdomą veiklą.

Kibernetinio saugumo valdymo modelio teisinio reguliavimo dimensijos trečiojo lygmens įgyvendinimas organizacijoje yra siejamas su teisinio reglamentavimo dimensijos integravimu ir sujungimu su kitomis kibernetinio saugumo valdymo modelio dimensijomis.

Apibendrinant kibernetinio saugumo valdymo modelio teisinio reguliavimo dimensijos priemonių įgyvendinimą, galima teigti, kad jos įgyvendinimo priemonių įdiegimas ir naudojimas organizacijoje siejamas su organizacijos siekiu reglamentuoti savo vidaus ir išorės aplinkos veiklą, narių pareigas, funkcijas bei atsakomybių sritis, tokiu būdu suteikiant galimybę efektyviau priešintis kibernetiniams incidentams.

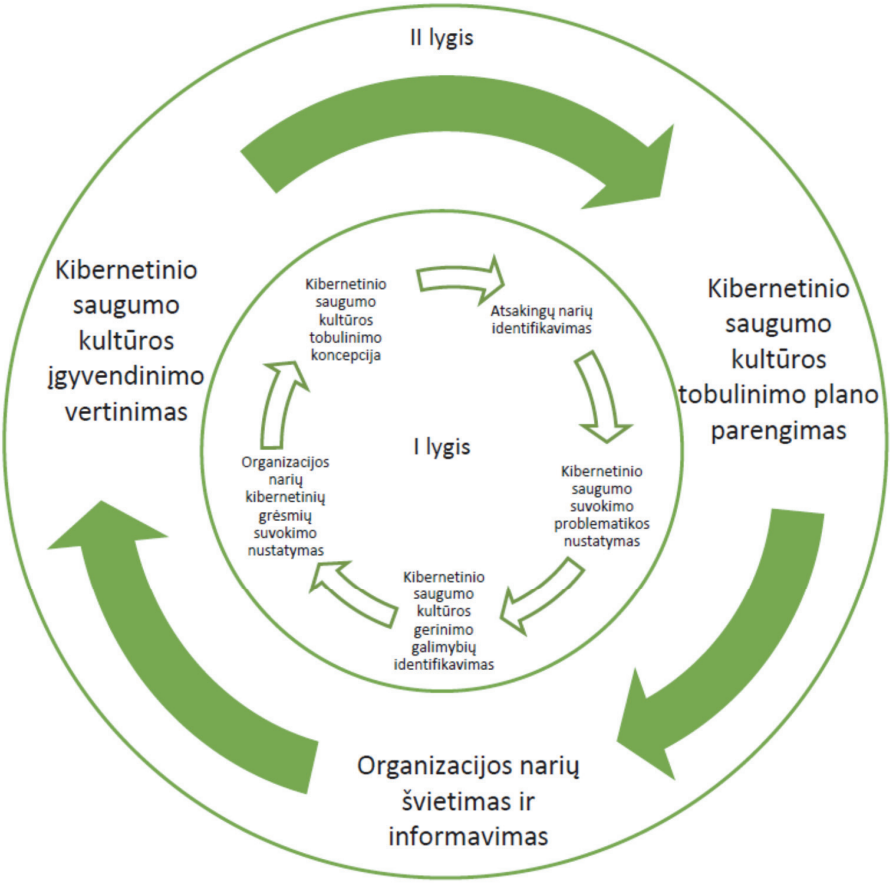
Organizacijos vidaus tvarkos taisyklės, pareiginės instrukcijos, tam tikras organizacijos narių vykdomų konkrečių pareigų reglamentavimas, darbų atlikimo taisyklės sudaro prielaidas išvengti netikėtumų kasdienėje organizacijos veikloje. Teisinio reglamentavimo dimensijos įgyvendinimo kontekste sukurtų organizacijos veiklos taisyklių rinkinys gali būti siejamas su išorinės teisinės aplinkos poveikiu organizacijai, tačiau organizacijos siekis reglamentuoti jos viduje vykstančius procesus suteikia organizacijai galimybę įgyti tam tikrą institucinę atmintį, sąlygojančią veiklos efektyvumo bei atsparumo ateities kibernetinėms grėsmėms padidėjimą.

3.2.4. Kibernetinio saugumo kultūros dimensijos analizė

Ši kibernetinio saugumo valdymo modelio dimensija yra skirta kibernetinio saugumo valdymo priemonėms, leisiančioms suvaldyti žmogiškojo faktoriaus įtaką organizacijos kibernetiniam saugumui, nagrinėti. Kitos kibernetinio saugumo valdymo dimensijų įgyvendinimo priemonės gali būti diegiamos organizacijoje, vadovaujantis parengtais planais, strateginio valdymo pokyčių būtinumu, atlikta teisinio reglamentavimo analize, rizikos vertinimo ataskaitomis, ekonominėmis prognozėmis ir skaičiavimais, o kibernetinio saugumo kultūros dimensijos priemonių įdiegimui būtinas aiškus organizacijos kibernetinio saugumo tradicijų ir vertybių įgyvendinimas, kibernetinių grėsmių suvokimo tarp organizacijos narių formavimas.

Kaip jau buvo minėta anksčiau ir kaip teigia mokslininkai, kibernetinio saugumo ekspertai ir kibernetinio saugumo sprendimus kuriančios ir diegiančios įmonės, vienas pagrindinių aspektų, sąlygojantis kibernetinius incidentus, yra žmogiškasis faktorius. Būtent žmogiškojo faktoriaus, emocijų, potyrių, pojūčių, norų ir nerūpestingumo įtaka kibernetiniam saugumui yra didžiausia, o visos organizacijos ir jos narių kibernetinio atsparumo galimybės priklauso nuo labiausiai pažeidžiamo organizacijos nario (Harrison, White, 2011; Alotaibi ir kt., 2016; Dunkelberg, 2017; Limba ir kt., 2017). Kibernetinio saugumo pagrindai, incidentų identifikavimo būdai, incidentų rūšys ir atakų vykdymo mechanizmai turi būti aiškiai suprantami kiekvienam organizacijos nariui, kadangi būtent šios mažos (ir dažnai nereikšmingos bei nereikalaujančios didelių investicijų) priemonės suteikia organizacijai galimybę aktyviai priešintis kibernetinėms atakoms ir kovoti už savo kibernetinį saugumą (Fernando, 2018).

Kibernetinio saugumo kultūros dimensija grafiškai yra pavaizduojama žemiau esančiame paveiksle (žr. 17 paveikslą).



Šaltinis: *Sudaryta autoriaus*

17 paveikslas. *Kibernetinio saugumo kultūros dimensija*

Toliau pateiktoje lentelėje (žr. 11 lentelę) yra išvardytos kibernetinio saugumo kultūros dimensijos priemonės, kurių įgyvendinimas organizacijoje padės efektyviai išvengti su šia dimensija siejamų kibernetinių grėsmių atsiradimo.

11 lentelė. *Kibernetinio saugumo kultūros dimensijos įgyvendinimo priemonės*

<table>
<tr><th colspan="3">Kibernetinio saugumo kultūros dimensija</th></tr>
<tr><th>1 lygis</th><th>2 lygis</th><th>3 lygis</th></tr>
<tr><td>Identifikuoti organizacijos narius, atsakingus už kibernetinio saugumo kultūros kūrimą.</td><td>Parengti ir patvirtinti organizacijos kibernetinio saugumo kultūros tobulinimo planą.</td><td rowspan="5">Kibernetinio saugumo kultūros dimensijos integravimas ir sujungimas su kitomis kibernetinio saugumo valdymo modelio dimensijomis.</td></tr>
<tr><td>Išanalizuoti didžiausias kibernetinio saugumo suvokimo tarp organizacijos narių problemas.</td><td rowspan="2">Vykdyti organizacijos narių švietimą ir informavimą.</td></tr>
<tr><td>Išanalizuoti organizacijos galimybes gerinti kibernetinio saugumo kultūrą.</td></tr>
<tr><td>Identifikuoti organizacijos narių kibernetinio saugumo ir kibernetinių grėsmių suvokimą.</td><td rowspan="2">Atlikti kibernetinio saugumo kultūros dimensijos plano įgyvendinimo vertinimą.</td></tr>
<tr><td>Parengti ir patvirtinti kibernetinio saugumo kultūros organizacijoje tobulinimo koncepciją.</td></tr>
</table>

Šaltinis: *Sudaryta autoriaus*

Siekdama tinkamo kibernetinio saugumo kultūros dimensijos įgyvendinimo organizacijoje, organizacija turi imtis tam tikrų priemonių įgyvendinimo. Šiai kibernetinio saugumo valdymo modelio dimensijai sklandžiai įgyvendinti organizacijoje būtinos pirmojo lygmens priemonės yra pateikiamos toliau:

- *Identifikuoti organizacijos narius, atsakingus už kibernetinio saugumo kultūros kūrimą*. Tai yra pirma kibernetinio saugumo kultūros dimensijos priemonė, kurios įgyvendinimas ateityje gali stipriai palengvinti visų tolimesnių šios dimensijos kūrimo priemonių panaudojimą organizacijoje. Vykdant kitų kibernetinio saugumo valdymo modelio dimensijų kūrimą organizacijoje, dažniausiai yra įmanoma vienareikšmiškai nustatyti, kokie organizacijos nariai bus atsakingi už tam tikros dimensijos priemonių įdiegimą ir gyvavimo ciklo kontrolę organizacijoje. Kibernetinio saugumo kultūros dimensija iš esmės skiriasi nuo kitų modelio dimensijų, kadangi už jos įgyvendinimą atsakingas ne vien tik organizacijos vadovaujanti grandis bei už konkrečių funkcijų įgyvendinimą atsakingas struktūrinis padalinys. Šiai dimensijai sėkmingai įgyvendinti turi būti suburta bendra specialistų komanda (darbo grupė), kurios nariai bus technologinių priemonių valdytojai, duomenų apsaugos specialistai, finansus valdančio padalinio atstovai bei personalo valdymo specialistai. Suburta komanda turi aiškiai suprasti, kokia yra jos misija ir kokius svarbius kibernetinio saugumo užtikrinimo klausimus ir problemas ji turės išspręsti. Tik tikslus ir išsamus užduočių suformulavimas bei kiekvieno komandos nario rolės bendroje komandoje suvokimas sudarys sąlygas

specialistams parengti ir įgyvendinti kibernetinio saugumo gerinimo priemonių planą, pagal kurį bus kuriama organizacijos kibernetinio saugumo valdymo modelio kibernetinio saugumo kultūros dimensija;

- *Identifikuoti organizacijos narių kibernetinio saugumo ir kibernetinių grėsmių suvokimą*. Šios priemonės įgyvendinimo metu organizacija turi aiškiai suprasti, kaip jos nariai (vidiniai ir išoriniai) supranta kibernetines grėsmes ir kokius savisaugos metodus naudoja, siekdami išvengti kibernetinių grėsmių. Pažymėtina, kad kibernetinio saugumo valdymas organizacijoje dažniausiai yra reglamentuojamas tam tikrais vidaus teisės aktais ir taisyklėmis, kurie apibrėžia organizacijos narių veiklą, teises bei atsakomybes, tačiau ne visuomet yra įmanoma pateikti teisinio reguliavimo normas visiems gyvenimo atvejams. Kaip jau buvo minėta anksčiau, žmogus yra laikomas silpniausia kibernetinio saugumo užtikrinimo grandimi, o kibernetinių incidentų sukėlėjai nenuilsdami stengiasi išnaudoti žmogaus silpnybes, vykdydami kibernetines atakas. Kibernetinių atakų sukėlėjai kombinuoja socialinės inžinerijos ir technologines atakas (Rao ir kt., 2016), stengiasi apgaule paveikti žmones ir tokiu būdu įsilaužti į organizacijų valdomą informacinę infrastruktūrą arba, organizacijai nežinant, rinkti informaciją apie organizacijos vykdomą veiklą. Kibernetiniai nusikaltėliai gali pasinaudoti organizacijos nariais ir įdiegti organizacijos naudojamuose duomenų perdavimo tinkluose technologines priemones (programinę įrangą), kuriomis pasinaudojant bus renkama informacija arba trikdoma organizacijos duomenų perdavimo tinklu įprastinė veikla. Pasaulyje yra žinomas ne vienas atvejis, kai programinės įrangos gamintojai (kompanijos) siūlydavo kompiuterių naudotojams nemokamą programinę įrangą. Ją įdiegus kompiuteriuose, vykdydavo vartotojų elgsenos internete analizę, siekdami personalizuoti vartotojams skirtą reklamą internete (Chang, 2016), ir atlikdavo neteisėtą organizacijos narių ir visos organizacijos veiklos procesų stebėjimą arba įvykdydavo konfidencialios informacijos vagystę iš organizacijos valdomų informacinių išteklių (Kenton, 2018; activetrak.com, 2019). Taip pasinaudoję socialinės inžinerijos atakų priemonėmis ir metodais, kibernetiniai nusikaltėliai sužinodavo prisijungimo prie organizacijos kompiuterinių išteklių duomenis ir įvykdydavo kibernetinius išpuolius prieš organizacijos informacinius išteklius ar interneto paslaugų naudotojus (Baxter, 2016). Socialinės inžinerijos panaudojimas, siekiant suklaidinti informacinių technologijų naudotojus, yra ne vienintelė priemonė, įgyvendinant kibernetines atakas. Dažnai vartotojai patys nesirūpina savo saugumu, asmeniniame gyvenime naudodami šiuolaikines informacines ir ryšių technologijas, o ilgainiui susiformuoja tam tikros technologijų naudotojų elgesio kibernetinėje erdvėje normos. Dabartiniu laikotarpiu kibernetinio saugumo produktų gamintojai, tarptautinės organizacijos ir mokslininkai, kalbėdami apie kibernetinio saugumo problemas, paveikiančias organizacija ir individus, atkreipia dėmesį į tai, kad pagrindiniu iššūkiu ir problema tampa netinkamas kibernetinio saugumo higienos suvokimas organizacijoje (ENISA, 2016; Trevors, Wallen, 2017; Haynes, 2019; Giniotienė, 2019). Kompiuterinių technologijų naudotojai ir už technologijų eksploataciją

atsakingų padalinių darbuotojai dažnai aplaidžiai vykdo savo pareigas, todėl organizacijos valdomi informaciniai ištekliai tampa pažeidžiami, o kibernetinių incidentų sukėlėjai, pasinaudodami susidariusia situacija ir technologinėmis žiniomis bei įgūdžiais, įvykdo sėkmingas kibernetines atakas. Dažniausiai pasitaikančios kibernetinio saugumo klaidos yra siejamos su netinkamu techninės ir programinės įrangos administravimu organizacijos viduje, neteisėtų duomenų saugojimo laikmenų ir neautorizuotos programinės įrangos naudojimu, neatsakingu prisijungimo prie informacinių išteklių duomenų (slaptažodžių) tvarkymu, netinkamu organizacijos išorinių narių kibernetinio saugumo situacijos suvokimu (Trevors, Wallen, 2017; Haynes, 2019). Siekdama sėkmingai įgyvendinti šią kibernetinio saugumo kultūros dimensijos pirmojo lygmens priemonę bei identifikuoti organizacijos narių ir išorinės aplinkos atstovų (tiekėjų, partnerių ir kt.) kibernetinio saugumo ir kibernetinių grėsmių suvokimą, organizacija privalo atlikti tyrimą, kurio metu turės išsiaiškinti tyrimo dalyvių grupių ir konkrečių narių požiūrį į kibernetinio saugumo problematiką;

- *Išanalizuoti didžiausias kibernetinio saugumo suvokimo tarp organizacijos narių problemas*, siekiant aiškiai įvardyti sritis, kuriose organizacijos narių kibernetinio saugumo kompetencijos yra mažiausios. Kibernetinio saugumo situacijos suvokimo problematikos išgryninimas ir prioritetinių sričių nustatymas gali suteikti organizacijai pakankamą kiekį informacijos, kuri bus naudinga kibernetinio saugumo kultūros dimensijos priemones įgyvendinant tolimesniuose kibernetinio saugumo valdymo organizacijoje įgyvendinimo etapuose. Vykdydama šios priemonės įgyvendinimą, organizacija turi suprasti, kad kiekvienai grupei (vartotojams, techninę ir programinę įrangą aptarnaujančiam personalui, išorinių paslaugų tiekėjams ir kt.) gali būti aktualūs skirtingi kibernetinio saugumo klausimai, ir, atsižvelgdama į tai, suformuoti skirtingą kibernetinio saugumo problematikos suvokimą ir sudaryti prioritetinių sričių sąrašą. Galima teigti, kad kompiuterinių paslaugų naudotojų kibernetinio saugumo suvokimo problematika bus susijusi su neaiškios paskirties arba nelegalios (piratinės) programinės įrangos naudojimu, nesaugių duomenų laikmenų naudojimu (asmeninės USB laikmenos, išoriniai standieji diskai ir kt.), nesaugių interneto svetainių naudojimu, netinkamu prisijungimo prie organizacijos informacinių išteklių duomenų saugojimu, neaiškių duomenų rinkmenų ir nuorodų į interneto svetaines, gautas elektroniniu paštu iš nežinomų šaltinių, atidarymu. Dažniausiai techninės ir programinės įrangos priežiūros specialistų nerūpestingumas yra susijęs su netinkamu prieigos teisių panaudojimu, vykdant kasdienius darbus, asmeninės techninės įrangos panaudojimu organizacijos informaciniams ištekliams administruoti, nerūpestingumu, vykdant techninės ir programinės įrangos sistemų atnaujinimus, savikontrolės priemonių ignoravimu (Haynes, 2019). Pažymėtina, kad kibernetinio saugumo kultūros dimensijos problematika yra aktuali ir išorinių paslaugų tiekėjams bei partneriams, tačiau jos įgyvendinimas dažniausiai nepriklauso nuo organizacijos. Organizacija, įgyvendinanti kibernetinio saugumo valdymo modelį, turi teisę (privalo) reikalauti iš savo partnerių

atlikti atitinkamus veiksmus ir įgyvendinti tam tikras priemones, kurios suteiktų partneriams galimybę pasiekti ne prastesnį kibernetinio saugumo lygį nei yra įgyvendintas pačioje organizacijoje;

- *Išanalizuoti organizacijos galimybes gerinti kibernetinio saugumo kultūrą*. Šios priemonės įgyvendinimo metu organizacija gali atlikti analizę, suteiksiančią organizacijai pakankamai žinių apie jos galimybes pagerinti kibernetinio saugumo kultūros dimensiją. Šios analizės metu organizacija gali įvertinti, ar ji turi pakankamai išteklių, kurių panaudojimas bus reikalingas šiai modelio dimensijai tobulinti. Nagrinėjant būtinų išteklių panaudojimo klausimą, turi būti įvertintos visos išteklių rūšys: finansiniai, žmogiškieji, infrastruktūros ir kt. Atlikusi organizacijos turimų pajėgumų vertinimą bei šio vertinimo rezultatus sujungusi su prieš tai esančios priemonės įgyvendinimo metu gautais rezultatais, organizacija turės aiškų susidariusios situacijos, susijusios su kibernetinio saugumo kultūros lygiu organizacijoje, matymą bei galės kitų priemonių įgyvendinimui tinkamai pasirengti. Galutinis šios priemonės įgyvendinimo rezultatas atspindės galimas organizacijos finansines išlaidas, personalo užimtumą, identifikuos klausimus ir problemas, kurias organizacija gali išspręsti, pasinaudodama savo vidiniais ištekliais, taip pat išgrynins organizacijai reikalingų išorinės aplinkos dalyvių teikiamų paslaugų kiekį bei šioms paslaugoms suteikti reikalingų finansinių išteklių poreikį;
- *Parengti ir patvirtinti kibernetinio saugumo kultūros organizacijoje tobulinimo koncepciją*, kurios pagrindinis tikslas yra siejamas su organizacijos galimybe, atsižvelgiant į dabartinę organizacijos būklę, egzistuojančias kibernetines grėsmes, turimus išteklius bei strateginius organizacijos tikslus, numatyti būsimą organizacijos kibernetinio saugumo kultūros dimensijos viziją, taip pat nusakyti, kaip ji atrodys ilgalaikėje perspektyvoje, kokios gali būti numatomos organizacijos kibernetinio saugumo kultūros dimensijos plėtros gairės bei etapai, prioritetinės sritys ir pagrindinės, būtinos išspręsti problemos. Rengdama anksčiau minėtą kibernetinio saugumo kultūros dimensijos tobulinimo koncepciją, organizacija turi aiškiai suvokti, kad šios koncepcijos parengimas reikalauja ypač daug dėmesio ir visų darbo grupės narių įsitraukimo, taip pat ši koncepciją turi būti suderinta su organizacijos sprendimų priėmėjų lygmeniu, nes organizacijos strateginių tikslų ir koncepcijos atitikimas ir tarpusavio suderinamumas užtikrina sėkmingą tolimesnį organizacijos kibernetinio saugumo kultūros dimensijos įgyvendinimą.

Organizacijai sėkmingai įgyvendinus kibernetinio saugumo valdymo modelio kibernetinio saugumo kultūros dimensijos pirmojo lygio priemones, organizacija turi imtis antrajame dimensijos lygmenyje išvardytų priemonių įgyvendinimo:

- *Parengti ir patvirtinti organizacijos kibernetinio saugumo modelio kibernetinio saugumo kultūros dimensijos tobulinimo planą*, kuriame yra aprašomi su dimensijos tobulinimu susiję veiksmai, numatoma jų įgyvendinimo seka bei aptariamos tokios svarbios sritys kaip: kibernetinio saugumo kultūros dimensijoje vykstančių procesų pokyčių valdymas, leisiantis aiškiai identifikuoti, kokie pokyčiai turi būti įgyvendinti organizacijoje, siekiant tobulinti kibernetinio saugumo kultūros

dimensijos įgyvendinimą; kibernetinio saugumo kultūros dimensijos pokyčiams įgyvendinti būtina organizacinė struktūra ir šios struktūros veiklos mechanizmai, atsakomybės sritis bei šių sričių valdymo dedikavimas tam tikriems organizacijos nariams; organizacijos personalo valdymo ir parengimo klausimai, nusakantys minimalius organizacijos personalo valdymo ir rengimo aspektus, personalo vadybos, mokymo ir tobulinimo metodus; kibernetinio saugumo kultūros dimensijai tobulinti būtinų materialių ir nematerialių išteklių poreikis, kuris nurodo dimensijai įgyvendinti būtinus kaštus bei šių kaštų panaudojimą. Organizacijos kibernetinio saugumo modelio kibernetinio saugumo kultūros dimensijos tobulinimo plane aprašoma konkreti, etapais suskirstyta kibernetinio saugumo kultūros dimensijos įgyvendinimo seka bei numatomas dimensijai įgyvendinti reikalingų materialinių išteklių gyvavimo ciklas, leisiantis konkrečiai prognozuoti šios dimensijos įgyvendinimo ir palaikymo kaštų poreikį;

- *Vykdyti organizacijos narių švietimą ir informavimą bei mokymą, siekiant įtraukti visus organizacijos narius į kibernetinio saugumo užtikrinimo procesą.* Šios priemonės įgyvendinimas yra siejamas su tinkamu ir laiku personalo parengimu. Kiekvienas organizacijos narys turi būti įtrauktas į organizacijos organizuojamus mokymus, siejamus su „kibernetinio saugumo higienos" (*angl. cyber hygiene)* palaikymu organizacijoje, bei periodiškai informuojamas apie dabartines kibernetinio saugumo raidos tendencijas globaliame pasaulyje. Tokie mokymai yra naudingi organizacijos nariams, kadangi taip yra ugdomas organizacijos narių sąmoningumas bei jų kibernetinio saugumo aplinkos suvokimas, o įgytos žinios ilgainiui tampa kasdieniais įpročiais, kurie būna naudingi ne tik asmeniniame organizacijos narių gyvenime, bet ir prisideda prie organizacijos kibernetinio saugumo situacijos gerinimo. Galima paminėti, kad Lietuvoje kibernetinio saugumo kultūros ugdymo problema yra žinoma ir labai aktuali, o vienas iš projektų, įgyvendinant kibernetinio saugumo kultūros dimensijos priemones, buvo vykdomas valstybės mastu, kai buvo organizuojami *Elektroninės informacijos saugos (kibernetinio saugumo) mokymai valstybės ir savivaldybių institucijų ir įstaigų dirbantiesiems.* Pažymėtina, kad organizacijos narių kibernetinio saugumo įgūdžių lavinimas yra siejamas ne tik su organizacijos narių, kasdien dirbančių su informacinių technologijų priemonėmis (kompiuteriais), mokymais, bet taip pat ir su personalo, vykdančio informacinių ir ryšių technologijų administravimo funkcijas organizacijoje, mokymais. Kiekvienas telekomunikacinių technologinių priemonių administratorius (bei jį pavaduojantis asmuo) turi būti apmokytas dirbti su jo atsakomybėje esančia technine ir programine įranga, žinoti šios įrangos konfigūravimo bei veikimo principus ir atliekamas funkcijas. Taip pat organizacijos personalo valdymo padalinys būtinai turi planuoti technologinio kibernetinio saugumo užtikrinimo įrangos specialistų mokymus bei kvalifikacijos tobulinimo kursus, siekdamas nuolat atnaujinti jų žinias ir atsižvelgdamas į kibernetinio saugumo situacijos kaitą organizacijos išorinėje aplinkoje bei kibernetinių grėsmių raidą globalioje aplinkoje. Įgyvendinant šią kibernetinio saugumo kultūros dimensijos priemonę organizacijoje bei vykdant organizacijos na-

rių mokymo ir informavimo procesą, gali būti naudojami organizacijos vidiniai ištekliai, jei, žinoma, organizacija yra pajėgi tai atlikti, arba gali būti samdomas išorinis paslaugų teikėjas, kuris turi pakankamai kompetencijų ir patirties šios priemonės įgyvendinimui užtikrinti;

- *Atlikti kibernetinio saugumo kultūros dimensijos tobulinimo plano įgyvendinimo vertinimą*, siekiant nustatyti, kaip anksčiau minėtų priemonių įgyvendinimas paveikė kibernetinio saugumo kultūros dimensiją organizacijoje. Šiame žingsnyje organizacija įgaus žinių, kaip pasirinktų priemonių įgyvendinimo procesas veikė organizacijos kibernetinio saugumo kultūrą bei kokios reikalingos šios dimensijos priemonių korekcijos. Vykdydama šios priemonės įgyvendinimo analizę, organizacija turi vadovautis savo sukurta veiklos efektyvumo vertinimo sistema, kuri bus aprašoma kitoje šio disertacinio darbo dalyje. Būtina pažymėti, kad organizacijoje galimi ir kitokie efektyvumo vertinimo modeliai, pvz.: vertinimas gali būti organizuojamas, imituojant kibernetinio saugumo incidentus organizacijoje ir vykdant organizacijos narių elgsenos stebėjimą. Imituojant kompiuterinio saugumo incidentus organizacijoje, galima pasinaudoti socialinės inžinerijos priemonėmis įgyvendinamomis kibernetinėmis atakomis, kurių metu siekiama priversti organizacijos narius atskleisti jų prisijungimo prie informacinių išteklių duomenis; atidaryti tam tikrus elektroniniu paštu pateiktus dokumentus ar nuorodas; darbo vietose panaudoti neaiškios kilmės duomenų laikmenas (pvz., kompaktinius diskus, USB laikmenas ir kt.). Rekomenduotina atlikti organizacijos kibernetinio saugumo kultūros vertinimo tyrimą, panaudojant socialinės inžinerijos kibernetinių atakų technologijas, dar prieš kibernetinio saugumo kultūros dimensijos organizacijoje tobulinimo plano parengimą ir organizacijos narių mokymų organizavimą, kadangi gauti rezultatai leis nustatyti organizacijos silpnąsias vietas. Taip pat pažymėtina, kad pradinio praktinio tyrimo rezultatai suteiks galimybę ateityje vienareikšmiškai įvertinti organizacijos kibernetinio saugumo kultūros dimensijos įgyvendinimo procesą. Apie pradinio tyrimo rezultatus nebūtina, o dažniausiai net ir nereikia, informuoti organizacijos narių. Rezultatų pristatymas organizacijos nariams turi būti atliekamas, tik atlikus pakartotiną tyrimą ir gautų rezultatų lyginamąją analizę. Pažymėtina, kad tokie tyrimai turi būti atliekami periodiškai, o jų rezultatai turi būti pateikiami apibendrinta forma, nuasmeninant gautus duomenis, kad nebūtų sukeltas stresas organizacijos nariams.

Kibernetinio saugumo kultūros dimensijos trečiojo lygmens įgyvendinimas organizacijoje, kaip ir visų kitų jau aptartų ir tolimesnėse šio disertacinio darbo dalyse aprašomų dimensijų įgyvendinimas, yra įmanomas tik tuomet, kai visose šešiose modelio dimensijose yra pasiektas antrasis lygmuo.

Apibendrinant kibernetinio saugumo kultūros dimensijos priemonių įdiegimą organizacijoje, galima pažymėti, kad pagrindinis šių priemonių įgyvendinimo tikslas yra iš esmės susijęs su organizacijos narių kibernetinio saugumo situacijos suvokimo ir sąmoningumo formavimu bei tam tikrų kasdienio kibernetinio saugumo higienos normų įskiepijimu. Organizacijos narių suvokimas, kad kibernetinėje erdvėje galioja tam

tikros saugaus elgesio taisyklės ir kad visos organizacijos pasirengimas kibernetinio saugumo užtikrinimui yra veikiamas kiekvieno nario kasdienio elgesio kibernetinėje erdvėje įpročių, suteikia organizacijai galimybę efektyviai kovoti su kibernetinių grėsmių sukėlėjais bei sėkmingai užkirsti kelią kibernetiniams incidentams.

3.2.5. Technologinio kibernetinio saugumo dimensijos analizė

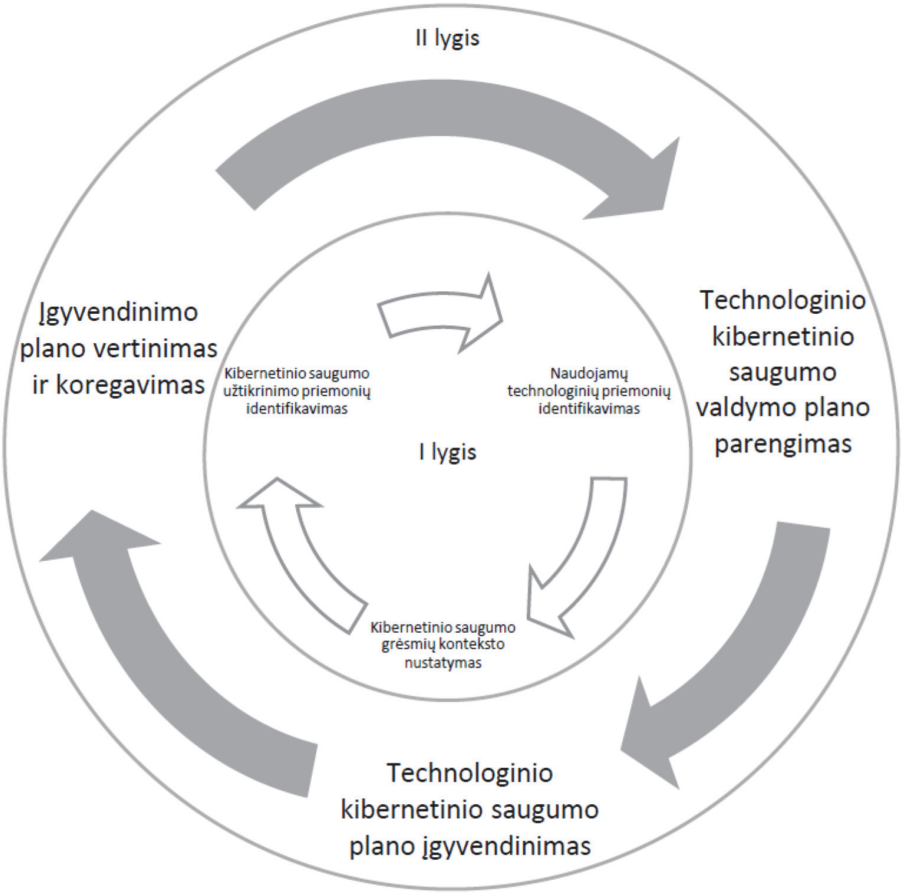
Kibernetinio saugumo reiškinio sąvoka dažniausiai yra tapatinama su technologiniais apsaugos sprendimais, kurie yra naudojami, siekiant apsaugoti organizacijos valdomus informacinius išteklius nuo galimų kibernetinių grėsmių, atakų ar įsibrovimo į organizacijos valdomą duomenų perdavimo infrastruktūrą. Technologinio kibernetinio saugumo priemones ir jų panaudojimo galimybes analizuoja kibernetinio saugumo ekspertai, mokslininkai ir kompanijos, kurių pagrindinis tikslas yra sukurti ir pateikti vartotojams apsaugos sprendimus, galinčius sumažinti kibernetinių incidentų atsiradimo galimybę organizacijų valdomoje informacinėje infrastruktūroje. Yra sukurta begalė technologinių kibernetinio saugumo užtikrinimo priemonių (programinė ir technologinė įranga), kibernetinio saugumo valdymo modelių (SANS instituto, NIST, $(ISC)^2$ ir kt.), taip pat standartų (ISO27001/27002, COBIT, PAS555), kurių panaudojimas organizacijos veikloje gali sumažinti kibernetinio saugumo incidentų atsiradimo tikimybę. Būtina pažymėti, kad, kaip jau buvo minėta anksčiau, kibernetinis saugumas yra daug platesnė sąvoka, apimanti ne tik technologinių priemonių panaudojimą, siekiant užkirsti kibernetinių incidentų atsiradimo galimybę, ir jos tapatinimas su technologiniu požiūriu į organizacijos valdomų išteklių saugumą yra klaidinantis ir nepriimtinas šiuolaikinių kibernetinių grėsmių kontekste (Solms, Niekerk, 2013; Campbell, 2017; Limba ir kt., 2017; Collier, 2018; E&Y, 2018).

Neabejotina, kad organizacijos kibernetinio saugumo valdymo proceso įgyvendinimas yra neįsivaizduojamas ir neįmanomas be šiuolaikiškų technologinių sprendimų (techninės ir programinės kibernetinio saugumo užtikrinimo įrangos, valdomų išteklių fizinės apsaugos sistemų ir kt.) panaudojimo, tačiau būtina pažymėti, kad šiame disertaciniame darbe kuriamo kibernetinio saugumo valdymo modelio technologinio kibernetinio saugumo dimensijoje nebus analizuojamos ar aptariamos konkrečios technologinės saugumo užtikrinimo priemonės, jų tarpusavio suderinamumo galimybės bei šių priemonių konfigūravimo aspektai. Kibernetinio saugumo priemonių įdiegimas organizacijoje priklauso nuo pačios organizacijos požiūrio į konkrečių technologinių priemonių panaudojimą, finansinių galimybių bei techninio personalo kvalifikacijos, nes tai yra tiesiog technologinis procesas, kuriam realizuoti gali būti panaudojami skirtingi sprendimai.

Šiame disertaciniame darbe technologinis kibernetinis saugumas bus analizuojamas per valdymo prizmę, siekiant akcentuoti organizacijos veiksmus, kurie yra būtini, kad technologinės kibernetinio saugumo priemonės būtų sklandžiai įgyvendintos. Organizacija ir jos nariai turi aiškiai suvokti, kad chaotiškas ir nekontroliuojamas technologinių priemonių panaudojimas organizacijos valdomų informacinių išteklių saugumui užtikrinti yra žalingas ne tik kibernetinio saugumo, bet ir finansinių sąnaudų požiūriu. Organizacija, atsižvelgdama į esamus ar planuojamus veiklos procesus,

vykdomą veiklą, infrastruktūrą, valdomų informacinių išteklių didį ir kitus svarbius organizacijos veiklą veikiančius aspektus, turi sukurti aiškią technologinio kibernetinio saugumo valdymo viziją, nusistatyti realius įgyvendinamus tikslus bei numatyti šių tikslų pasiekimo būdą. Visi anksčiau išvardyti veiksmai ilgainiui suteiks organizacijai galimybę tinkamai valdyti technologinio kibernetinio saugumo priemones, tokiu būdu užtikrinant organizacijos informacinių išteklių apsaugą bei sumažinant kibernetinio saugumo incidentų atsiradimo tikimybę.

Technologinio kibernetinio saugumo dimensija grafiškai yra pavaizduojama žemiau esančiame paveiksle (žr. 18 paveikslą).



Šaltinis: *Sudaryta autoriaus*

18 paveikslas. *Technologinio kibernetinio saugumo dimensija*

Toliau pateiktoje lentelėje (žr. 12 lentelę) yra pateiktos kibernetinio saugumo valdymo modelio technologinio kibernetinio saugumo valdymo priemonės, kurių įgyvendinimas organizacijoje padės efektyviai valdyti organizacijos naudojamas technologines saugumo priemones, siekiant minimizuoti kibernetinio saugumo incidentų atsiradimo organizacijos infrastruktūroje tikimybę.

12 lentelė. *Technologinio kibernetinio saugumo dimensijos įgyvendinimo priemonės*

<table>
<tr><th colspan="3">Technologinio kibernetinio saugumo dimensija</th></tr>
<tr><th>1 lygis</th><th>2 lygis</th><th>3 lygis</th></tr>
<tr><td>Atlikti visų organizacijos veiklos procesuose naudojamų technologinių priemonių identifikavimą.</td><td rowspan="2">Parengti organizacijos technologinio kibernetinio saugumo valdymo planą.</td><td rowspan="3">Technologinio kibernetinio saugumo dimensijos integravimas ir sujungimas su kitomis kibernetinio saugumo valdymo modelio dimensijomis.</td></tr>
<tr><td>Nustatyti kibernetinio saugumo grėsmių organizacijai kontekstą.</td></tr>
<tr><td>Identifikuoti visas galimas technologines kibernetinio saugumo užtikrinimo priemones.</td><td>Atlikti technologinio kibernetinio saugumo valdymo plano įgyvendinimo organizacijoje įvertinimą ir koregavimą.</td></tr>
</table>

Šaltinis: *Sudaryta autoriaus*

Sklandžiam technologinio kibernetinio saugumo dimensijos įgyvendinimui organizacijoje, būtina imtis toliau pateiktų pirmojo lygmens priemonių įgyvendinimo:

- *Atlikti visų organizacijos veiklos procesuose naudojamų technologinių priemonių identifikavimą*, siekiant nustatyti, kokie techniniai ir programiniai sprendimai (įrenginiai) yra naudojami įmonės veiklai užtikrinti ir verslo procesams vykdyti. Šios priemonės įgyvendinimo metu organizacija turi aiškiai nustatyti visus jos valdomus materialiuosius išteklius, jų buvimo vietą bei organizacijos narių ar kitų asmenų prieigos galimybę prie valdomų išteklių, taip pat identifikuoti verslo procesus, kuriems vykdyti gyvybiškai reikalinga tam tikra technologinė kibernetinio saugumo užtikrinimo įranga. Pažymėtina, kad šios priemonės įgyvendinimas (tikslus valdomų išteklių ir atsakingų šių išteklių valdytojų identifikavimas) suteikia organizacijai galimybę aiškiai suvokti būtinos saugoti technologinės įrangos kiekį, jos buvimo vietą ir ją valdančius (už naudojimą atsakingų) organizacijos narius, tokiu būdu stipriai sumažinant tolimesnę šios dimensijos priemonių įgyvendinimo problematiką. Šios technologinio kibernetinio saugumo dimensijos priemonės įgyvendinimas organizacijoje gali būti vykdomas keliais etapais:
  - Pradinis technologinių priemonių identifikavimas, kurio metu yra sudaromas visos techninės ir programinės įrangos, naudojamos organizacijoje, aprašo-

masis žinynas (sąrašas), nurodant jos buvimo vietą, patekimo prie įrangos galimybes ir kt.;

- Identifikuoto technologinės įrangos valdytojo nustatymas, apibrėžiantis, koks organizacijos padalinys ar organizacijos narys yra atsakingas už minėtos įrangos valdymą bei kontrolę. Šiame etape identifikuotas technologinės įrangos valdytojas gali aiškiai nurodyti, kokia yra konkrečios technologinės įrangos paskirtis, taip pat suteikti organizacijai informaciją, kokiems organizacijos veiklos procesams užtikrinti reikalingas kiekvienas jo valdomas turtas;
- Technologinės įrangos įtakos organizacijos veiklos procesams nustatymas, kurio metu yra įvardijamas technologinės įrangos elementų panaudojimo faktas organizacijos veikloje. Šiame etape būtina aiškiai identifikuoti visus organizacijos veiklos procesus ir jiems vykdyti būtinus technologinius išteklius, kadangi vykdomų procesų ir panaudojamos įrangos tarpusavio ryšių identifikavimas gali padėti nustatyti kritinius aspektus organizacijos veiklos tęstinumui užtikrinti;
- Technologinių elementų tarpusavio ryšių nustatymas, suteikiantis organizacijai galimybę apibrėžti galimą technologinių priemonių tarpusavio sąveiką. Šio etapo metu sudaryti sąrašai aiškiai nusakys, kokie technologiniai sprendimai, naudojami organizacijos veikloje, yra tarpusavyje priklausomi, o jų veiklos sutrikimai (kibernetinės atakos) gali stipriai veikti organizacijos veiklos procesus.

Atlikusi anksčiau aprašytą technologinių priemonių identifikavimą, organizaciją galės vienareikšmiškai nustatyti didžiausią vertę turinčią technologinę įrangą, kurios apsauga nuo kibernetinio saugumo grėsmių (taip pat funkcionalumo laiku atstatymas po kibernetinio saugumo incidentų) užtikrins nepertraukiamą organizacijos veiklą;

- *Nustatyti kibernetinio saugumo grėsmių organizacijai kontekstą*, siekiant aiškiai įvardyti galimai pažeidžiamus organizacijos valdomus technologinius sprendimus bei numatyti galimą žalą organizacijai incidento atsiradimo atveju. Įgyvendindama šią priemonę, organizacija turi naudotis anksčiau aprašytos priemonės įgyvendinimo metu surinktais duomenimis, kurie vienareikšmiškai nusako, kokia technologinė organizacijos valdoma įranga turi didžiausią įtaką organizacijos veiklos tęstinumo užtikrinimui. Pažymėtina, kad šios priemonės įgyvendinimo metu turi būti vertinamas ne tik technologinių išteklių (techninės ir programinės įrangos) atsparumas kibernetinėms grėsmėms, bet ir fizinis poveikis (neteisėta prieiga prie infrastruktūros, vagystė ir kt.) organizacijos valdomiems ištekliams. Organizacija, atlikusi kibernetinių grėsmių konteksto nustatymą ir aiškiai įvardinusi grėsmių technologiniams sprendimams pobūdį ir galimus pažeidžiamumų realizavimo metodus, galės sudaryti pažeidžiamos technologinės įrangos žinyną. Pažymėtina, kad kuo tiksliau ir išsamiau bus įvardytos grėsmės, aprašyti galimų kibernetinių atakų realizavimo būdai, taip pat fizinės saugos pažeidžiamumai bei kiti aspektai, galintys per technologinę įrangą veikti organizacijos veiklą, tuo paprasčiau bus įgyvendinama kita kibernetinio saugumo valdymo modelio technologinio kibernetinio saugumo valdymo dimensijos priemonė;

- *Identifikuoti visas galimas technologines kibernetinio saugumo užtikrinimo priemones*, kurių panaudojimas padidins organizacijos kibernetinio saugumo lygį, taip pat užtikrins organizacijos vykdomų veiklos procesų tęstinumą. Įgyvendinant šią technologinio kibernetinio saugumo dimensijos priemonę organizacijoje, patartina suskirstyti visas galimas kibernetinio saugumo užtikrinimo priemones į tris grupes, atsižvelgiant į jų atliekamas funkcijas:
- Fizinės apsaugos priemonės, kurios yra naudojamos organizacijos valdomų išteklių apsaugai nuo neteisėtos prieigos, pagrobimo, sugadinimo ir kitų grėsmių. Prie šių apsaugos priemonių gali būti priskiriamos vaizdo stebėjimo, įeigos kontrolės ir kitos apsaugos sistemos, kurios sumažina technologinės įrangos pasiekiamumą kibernetinių incidentų sukėlėjams, apsunkindamos ne tik galimybę fiziškai paveikti technologinę įrangą, bet ir galimybę, pasinaudojant neteisėta prieiga, įdiegti kenkėjišką programinę įrangą į organizacijos valdomus duomenų perdavimo tinklo elementus, taip paveikiant organizacijos įprastinę veiklą;
- Techninės ir programinės įrangos apsaugos priemonės, kurios naudojamos, siekiant užtikrinti organizacijos valdomų duomenų perdavimo tinklų ir technologinės (techninės ir programinės) įrangos saugumą. Šiai grupei gali būti priskiriami duomenų perdavimo tinklo saugumo įrenginiai (ugniasienės, maršrutizatoriai, komutatoriai ir kt.), programinė įranga, atsakinga už darbo (vartotojų kompiuterių) ir tarnybinių stočių (serverių) saugumą (antivirusinė programinė įranga, vartotojų prisijungimo duomenų kontrolės programiniai sprendimai ir kt.), perduodamų duomenų šifravimo programinė ir techninė įranga (šifratoriai) ir kiti kibernetinio saugumo užtikrinimo technologiniai sprendimai, kuriuos siūlo kibernetinio saugumo užtikrinimo produktų gamintojai. Pagrindinis šiai grupei priskiriamos įrangos uždavinys yra apsaugoti visą technologinę organizacijos valdomą įrangą nuo technologinių kibernetinių atakų, kurios gali būti vykdomos prieš organizacijos valdomą informacinę infrastruktūrą;
- Informacinių ir telekomunikacinių technologijų įprastinės veiklos stebėjimo priemonės, kurios yra naudojamos organizacijos informaciniuose ištekliuose, siekiant identifikuoti neįprastą (įtartiną) technologinės įrangos (kompiuterių) ir duomenų perdavimo įrenginių veikimą. Šiai grupei gali būti priskiriama technologinė ir programinė įranga, informuojanti organizacijos atsakingą personalą apie duomenų perdavimo tinklo anomalijas, netipiškus įvykius ar įtartinus duomenų srautus organizacijos valdomame duomenų perdavimo tinkle.

Pažymėtina, kad, identifikuodama galimas technologinio kibernetinio saugumo užtikrinimo priemones, organizacija turi atsižvelgti į savo vykdomos veiklos ypatumus ir technologijų įtaką organizacijos veiklos procesams, nes nuo to priklauso galimų kibernetinio saugumo užtikrinimo priemonių panaudojimo tikslingumas ir sudėtingumas.

Po sėkmingo technologinio kibernetinio saugumo dimensijos pirmojo lygmens priemonių įgyvendinimo organizacija turi pradėti įgyvendinti antrajame dimensijos lygyje išvardytas priemones:

- Parengti organizacijos technologinio kibernetinio saugumo valdymo planą, kuris suteiks organizacijai galimybę aiškiai nusakyti technologinio kibernetinio saugumo valdymo strategiją, identifikuoti technologinio kibernetinio saugumo įgyvendinimo tikslus bei nurodys, kokias saugumo priemones būtina panaudoti organizacijos kibernetiniam saugumui užtikrinti. Pažymėtina, kad į technologinio kibernetinio saugumo valdymo plano parengimo procesą turi būti įtraukti visi suinteresuoti organizacijos nariai (pvz., informacinių technologijų departamentas, finansų departamentas ir kt.). Pasinaudojant kibernetinio saugumo valdymo modelio technologinio kibernetinio saugumo dimensijos pirmojo lygmens priemonių įgyvendinimo metu surinktais duomenimis, taip pat atsižvelgiant į organizacijos jau turimas ir naudojamas saugumo užtikrinimo priemones, turi būti sudarytas technologinio kibernetinio saugumo valdymo planas, apibrėžiantis visas organizacijos nustatytas ir pasirinktas priemones, jų panaudojimo tikslą, planuojamą įdiegimo laiką, finansavimo šaltinius ir kt. Pažymėtina, kad technologinio kibernetinio saugumo valdymo plano sudarymas yra labai svarbus, nes tik jis gali aiškiai identifikuoti organizacijos veiklos procesams užtikrinti, būtinos technologinės įrangos veikimui užtikrinti reikalingas saugumo priemones, įrangos gyvavimo ciklą, atnaujinimo ar pakeitimo prioritetus bei daugelį kitų dalykų. Šis organizacijos parengtas planas suteikia organizacijai galimybę nuo chaotiško kibernetinio saugumo pereiti prie tikslingo, į rezultatus orientuoto technologinio saugumo valdymo, kurio tikslai yra nustatyti, atsižvelgiant į organizacijos supančias vidaus ir išorės aplinkas, globalias kibernetinių grėsmių kaitos tendencijas bei organizacijos veiklos pobūdį ir joje vykstančius procesus;
- Atlikti technologinio kibernetinio saugumo valdymo plano įgyvendinimo organizacijoje įvertinimą ir koregavimą. Šios priemonės įgyvendinimo metu organizacija galės nustatyti, kaip anksčiau minėtų technologinio kibernetinio saugumo valdymo dimensijos priemonių įgyvendinimas yra vykdomas organizacijoje, taip pat kaip jos veikė technologinio kibernetinio saugumo valdymą organizacijoje. Pažymėtina, kad technologinio kibernetinio saugumo valdymo plano vertinimas ir jo korekcijos turi būti atliekamos periodiškai, kadangi tik tokiu būdu galima užtikrinti, kad organizacijos veiksmai, susiję su technologinio kibernetinio saugumo užtikrinimu, bus atlikti laiku ir vis dar aktualūs bei reikalingi, siekiant užtikrinti kibernetinio saugumo situacijos organizacijoje tobulinimą.

Kibernetinio saugumo valdymo modelio technologinio kibernetinio saugumo dimensijos trečiojo lygmens įgyvendinimas organizacijoje yra siejamas su organizacijos kibernetinio saugumo valdymo reiškinio virsmu į tam tikrą integruotą modelį, kuriame visos šiame disertaciniame darbe minimos kibernetinio saugumo valdymo modelio dimensijos tampa tiesiogiai priklausomos viena nuo kitos.

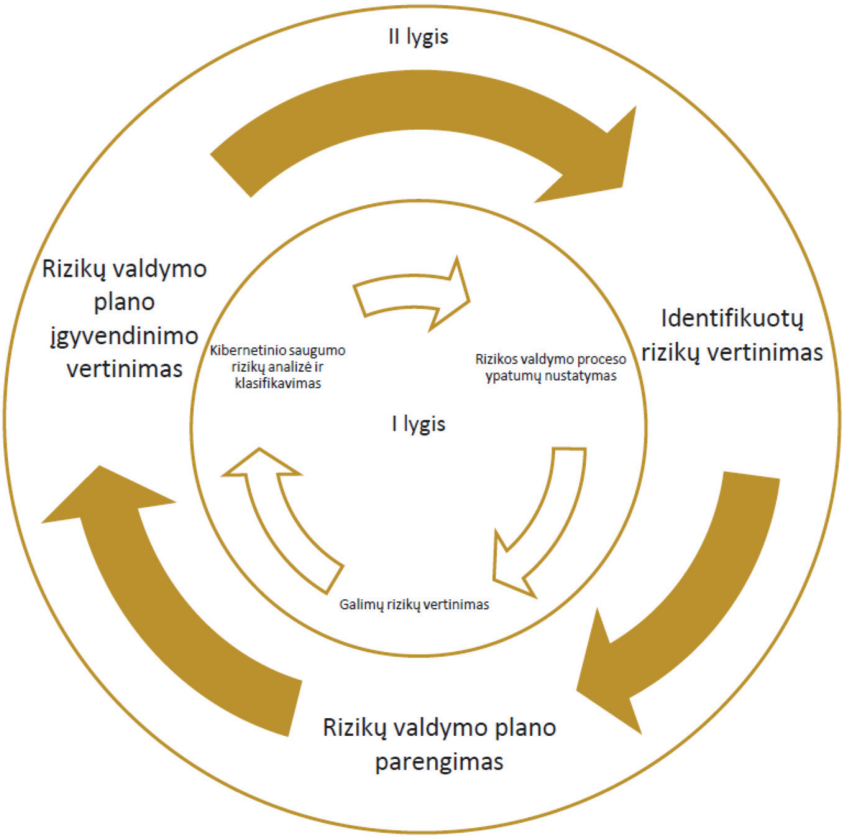
Apibendrinant galima teigti, kad šiame disertaciniame darbe nagrinėjama technologinio kibernetinio saugumo valdymo dimensija yra siejama ne tik su technologinių priemonių panaudojimu organizacijoje (kas tiesiog negali būti ginčijama), bet didžiausias dėmesys šioje dimensijoje yra siejamas su būtinybe organizacijai įgyti tam tikras kompetencijas ir žinias, kurios padės pačiai organizacijai suprasti technologinio

kibernetinio saugumo valdymo taisykles bei prioritetus. Grėsmių ir kibernetinių pavojų suvokimas organizacijoje suteikia jai galimybę, tikslingai panaudojant technologinius sprendimus, mažinti kylančias grėsmes ir didinti atsparumą kibernetiniams pažeidžiamumams.

3.2.6. Rizikos valdymo dimensijos analizė

Kibernetinio saugumo valdymo modelio dimensija, nagrinėjanti organizacijos gebėjimą tinkamai identifikuoti jos vidinės ir išorinės aplinkos rizikas, užtikrina, kad organizacija yra įgijusi pakankamai žinių ir turi tam tikrus specialius gebėjimus bei procedūras, suteikiančias jai galimybę kontroliuoti šių rizikų poveikį organizacijoje vykstantiems veiklos procesams. Pasaulio mokslininkai pažymi, kad, vykdydama savo veiklą, organizacija neturi galimybių išvengti išorinės ir vidinės aplinkos sukeliamų pavojų ir juos eliminuoti, bet daug svarbesnis dalykas slypi organizacijos gebėjime nustatyti galimas rizikas ir parengti veiksmų planus, suteiksiančius organizacijai galimybes maksimaliai sumažinti rizikų atsiradimo ir kibernetinio saugumo incidentų padarinius (Shedden ir kt., 2011; O'Neill, 2017; Vega ir kt., 2017; Patiño ir kt., 2018; Patiño, Yoo, 2018). Kitaip tariant, viena iš pagrindinių organizacijos užduočių yra ne vien tik išmokti vengti aplinkos veiksnių keliamų rizikų ir mokėti joms pasipriešinti, bet mokėti jas tinkamai identifikuoti ir suvaldyti. Rizikos valdymo ir galimų rizikų identifikavimo gebėjimo vystymas organizacijoje suteikia jai pranašumą bei galimybę tinkamai prisitaikyti prie kintančių organizacijos vidaus ir išorės aplinkose atsirandančių rizikų, tokiu būdu eliminuodamas organizacijos narių įpročius mechaniniu būdu valdyti anksčiau nustatytas rizikas, nevykdant naujai atsirandančių grėsmių analizės ir rizikų atsiradimo prognozavimo proceso.

Rizikos valdymo dimensija grafiškai yra pavaizduojama žemiau esančiame paveiksle (žr. 19 paveikslą).



Šaltinis: *Sudaryta autoriaus*

19 paveikslas. *Rizikos valdymo dimensija*

Sėkmingas kibernetinio saugumo rizikos valdymo dimensijos priemonių įgyvendinimas organizacijoje suteikia organizacijai galimybę išvengti daugumos egzistuojančių kibernetinių grėsmių ir pažeidžiamumų, taip pat numatyti galimų kibernetinių incidentų atsiradimą organizacijos valdomuose ištekliuose. Pasak pasaulio mokslininkų ir tarptautinių organizacijų, rizikos valdymas turi apimti visą organizaciją ir jos išorinę bei vidinę aplinkas, o tikslus rizikos valdymo priemonių nustatymas ir įgyvendinimas organizacijoje yra būtinas sėkmingai organizacijos veiklai užtikrinti (LST, 2011; Chen ir kt., 2014; IRM, 2017; Limba ir kt., 2017; Shamala ir kt., 2017; Vega ir kt., 2017; Patiño, Yoo, 2018).

Toliau pateiktoje lentelėje (žr. 13 lentelę) yra pateikiamos kibernetinio saugumo valdymo modelio rizikos valdymo dimensijos priemonės, kurių įgyvendinimas organizacijai padės efektyviai išvengti su šia dimensija siejamų kibernetinių grėsmių atsiradimo.

13 lentelė. *Kibernetinio saugumo rizikos valdymo dimensijos įgyvendinimo priemonės*

Kibernetinio saugumo rizikos valdymo dimensija		
1 lygis	**2 lygis**	**3 lygis**
Identifikuoti ir nustatyti kibernetinio saugumo rizikos valdymo proceso ypatumus organizacijos kontekste.	Atlikti identifikuotų kibernetinio saugumo rizikų vertinimą.	Kibernetinio saugumo rizikos valdymo dimensijos integravimas ir sujungimas su kitomis kibernetinio saugumo valdymo modelio dimensijomis.
Atlikti galimų kibernetinio saugumo rizikų organizacijoje vertinimą.	Parengti organizacijos kibernetinio saugumo rizikų valdymo planą.	
Atlikti organizacijos kibernetinio saugumo rizikų analizę ir klasifikavimą.	Atlikti kibernetinio saugumo rizikos valdymo plano įgyvendinimo organizacijoje įvertinimą.	

Šaltinis: *Sudaryta autoriaus*

Kad kibernetinio saugumo rizikos valdymo dimensija organizacijoje būtų sklandžiai įgyvendinta, organizacija turi įgyvendinti toliau pateikiamas pirmojo lygmens priemonės:

- *Identifikuoti ir nustatyti kibernetinio saugumo rizikos valdymo proceso ypatumus organizacijos kontekste,* siekiant suteikti organizacijai pakankamai žinių ir galimybių tinkamai organizuoti rizikos valdymo procesą, atsižvelgiant į organizaciją supančias vidaus ir išorės aplinkas. Šios priemonės įgyvendinimo metu taip pat turi būti aiškiai identifikuoti galimų rizikų valdymo kriterijai, apimtys ir apribojimai bei nustatyti organizacijos veiklos sritys ir veiklos procesai, susiję su rizikos valdymu organizacijoje (Agrawal ir kt., 2014; ISO, 2018). Organizacijai nustatant rizikos valdymo proceso ypatumus, turi būti aiškiai identifikuojami ištekliai, kurie bus būtini, vykdant rizikos valdymą organizacijoje (personalas, materialiniai ištekliai ir kt.), o organizacijos aukščiausios grandies vadovai turi aiškiai suprasti, kad rizikos valdymas yra sudėtingas procesas, reikalaujantis visapusiško organizacijos vadovybės palaikymo. Taip pat būtina pažymėti, kad rizikos valdymo dimensijos priemones įgyvendinantys organizacijos nariai turi turėti pakankamai žinių ir kompetencijų bei patirties vertinti galimas rizikas, kurias veikia organizacijos vidaus ir išorės aplinkos, nustatyti rizikos vertinimo metodiką ir vertinimo kriterijus, vykdyti nuolatinį rizikų valdymo proceso stebėjimą, pasirinkti rizikos valdymo metodus, nustatyti rizikos vertinimo kriterijus, galimų rizikų įtaką organizacijai ir joje vykstantiems veiklos procesams bei rizikų toleravimo ribas. Įgyvendindama šią kibernetinio saugumo rizikos vertinimo dimensijos priemonę, organizacija taip pat turi nustatyti rizikos valdymo dimensijos ribas ir apimtis, siekdama užtikrinti, kad rizikos valdymo procesas apims visas organizacijai svarbias sritis ir tuo pačiu nebus analizuojamos rizikos, kurios nesusijusios su organizacijos veikla arba kurių atsiradimas yra

nebūdingas organizacijai. Nustatant rizikos valdymo apimtis ir ribas, organizacijoje ypatingas dėmesys turi būti atkreiptas į organizacijos valdymą, veiklos procesus, organizacijos struktūrą, teisinio reguliavimo organizacijoje aspektus, išteklius bei organizaciją supančias aplinkas. Nustatant rizikos valdymo tikslus ir apribojimus organizacijoje, patartina atskirti rizikos valdymo sritis ir kiekvienai anksčiau įvardytai sričiai atlikti atskirą rizikos vertinimą, taip supaprastinant rizikos valdymo procesą. Pagrindinis šios rizikos valdymo dimensijos priemonės įgyvendinimo tikslas yra siejamas su organizacijos galimybėmis identifikuoti organizacijai tinkantį rizikos valdymo mechanizmą; nustatyti visus rizikos valdymo procese dalyvaujančius organizacijos narius; įvertinti išorinės ir vidinės aplinkos poveikį organizacijai bei organizacijos įtaką šioms aplinkoms; sukurti tinkamus organizacijos ir rizikos valdymo procese dalyvaujančių suinteresuotų narių bendradarbiavimo mechanizmus; parengti organizacijos rizikos valdymo procesą reglamentuojančias taisykles;

- *Atlikti galimų kibernetinio saugumo rizikų organizacijoje identifikavimą,* nustatant ir aprašant visas galimas rizikas organizacijoje. Įgyvendinant šią priemonę, patartina naudotis prieš tai esančios dimensijos priemonės įgyvendinimo metu nustatytomis rizikos valdymo sričių apimtimis (valdymo, išteklių, procesų ir kt.), taip supaprastinant rizikos valdymo proceso eigą organizacijoje. Šios priemonės vykdymo metu turi būti identifikuotos, taip pat prioretizuotos visos rizikos, būdingos tam tikrai organizacijoje egzistuojančiai rizikos valdymo sričiai. Būtina paminėti, kad, vykdant egzistuojančių ar galimai atsirasiančių kibernetinio saugumo rizikų organizacijoje vertinimą, patariama naudoti bent jau dviejų pakopų rizikos vertinimo procesą: pradinio vertinimo metu nustatomos reikšmingiausios (sudėtingiausios) rizikos, galinčios labiausiai veikti organizaciją ar jos veiklos procesus; antrinio vertinimo metu yra atliekama išsamesnė nustatytų reikšmingiausių rizikų analizė, suteikianti galimybę tinkamai įvertinti šių rizikų grėsmes ir reikšmingumą. Dviejų pakopų rizikų vertinimo procesas gali suteikti organizacijai didesnį suvokimą apie egzistuojančias rizikas ir jų sukeliamas grėsmes, kadangi vertinimo procese gali būti panaudojami skirtingi vertinimo metodai, o rizikos įtaka organizacijai ir rizikos svarba gali būti išmatuojama tiksliau. Įgyvendinusi šią pirmojo lygio priemonę, organizacija turi turėti baigtinį prioretizuotą įvertintų rizikų sąrašą, kuriame atsispindėtų kiekvienos rizikos poveikis konkrečiai organizacijos veiklos sričiai (valdymas, ištekliai, procesai ir kt.); sukeliamos grėsmės ir šių grėsmių įtaką organizacijoje; egzistuojančios rizikos valdymo galimybės (techninės priemonės, administracinės priemonės ir kt.); sukeliami padariniai (poveikis procesams, finansiniai praradimai, reputacijos praradimas ir kt.);
- *Atlikti organizacijos kibernetinio saugumo rizikų analizę ir klasifikavimą,* siekiant nustatyti visas galimas rizikas bei jų įtakos organizacijai mastą ir svarbą. Atliekamos rizikos analizės detalumas organizacijoje, priklauso nuo organizacijos keliamų rizikos valdymo tikslų ir dažniausiai yra nustatomas rizikos valdymo grupės narių, atsižvelgiant į organizacijos valdomų išteklių svarbą

organizacijos veiklai, žinomų kibernetinių pažeidžiamumų ir grėsmių organizacijai kiekį, ir, žinoma, į kibernetinio saugumo incidentus, kurie galimai yra įvykę organizacijos veikloje bei yra aiškiai identifikuoti. Vykdant rizikos analizę, gali būti naudojamas kiekybinis ar kokybinis rizikos analizės metodas arba šie metodai gali būti derinami tarpusavyje (Ackermann, 2012; LSD, 2018), atsižvelgiant į šiame kibernetinio saugumo valdymo dimensijos lygmenyje nustatytus rizikos valdymo proceso ypatumus organizacijoje. Organizacijai identifikavus visas galimas rizikas, šių rizikų atsiradimo aplinkybes ir poveikio sritis bei įvertinus šių rizikų poveikio mastą organizacijai (ištekliams, veiklos procesams ar kt.), turi būti atliktas visų rizikų klasifikavimas bei sudaromas galimų incidentų sąrašas, visapusiškai ir vienareikšmiškai identifikuojantis incidentus bei detalią kiekvienos rizikos įtaką organizacijai galimo incidento metu. Šios kibernetinio saugumo valdymo dimensijos priemonės įgyvendinimo metu taip pat turi būti vertinama rizikos atsiradimo tikimybė tam tikro kibernetinio atsiradimo metu bei rizikos priimtinumo organizacijai kriterijus (LSD, 2018). Sujungusi visus šios priemonės metu surinktus duomenis, organizacija įgaus žinių ir gebėjimų, kurie leis jai tinkamai įvertinti rizikas, jų atsiradimo tikimybę, poveikio organizacijai mastą, atsiradimo tikimybę ir kt., taip pat suteiks galimybę aiškiai suvokti, kokios rizikos ir kokiais būdais gali paveikti kasdienę organizacijos veiklą.

Organizacijai įgyvendinus kibernetinio saugumo valdymo modelio kibernetinio saugumo rizikos valdymo dimensijos priemones, išvardytas pirmajame lygyje, organizacija turi imtis antrajame dimensijos lygmenyje esančių priemonių įgyvendinimo:

- *Atlikti identifikuotų kibernetinio saugumo rizikų vertinimą*, kuris suteiks organizacijai galimybę nustatyti galimus organizacijos veiksmus, siekiant suvaldyti visas pirmajame rizikos valdymo dimensijos lygmenyje identifikuotas rizikas, taip pat pasirengti rizikos valdymo plano parengimui. Pažymėtina, kad pirmajame kibernetinio saugumo valdymo modelio rizikos dimensijos lygmenyje identifikuotas rizikas organizacija gali valdyti, pasinaudodama keturiomis rizikos valdymo technikomis: rizikos (modifikavimo) mažinimo, rizikos išlaikymo, rizikos vengimo ir rizikos paskirstymo (LSD, 2011; Ackermann, 2012; Agrawal ir kt., 2014). Pažymėtina, kad organizacija, vykdydama rizikos vertinimą, turi būtinai atsižvelgti į anksčiau įgyvendintų rizikos valdymo priemonių rezultatus bei pasirinkti tinkamas rizikos valdymo technikas konkrečioms organizacijos veiklos sritims. Be jokių abejonių galima teigti, kad skirtingose organizacijos veiklos srityse gali būti naudojamos skirtingos rizikų valdymo technikos, tačiau, pasirenkant techniką, būtina atsižvelgti į nustatytus rizikos valdymo proceso ypatumus organizacijoje, rizikos mažinimo priemonių kaštų apskaičiavimo rezultatus bei į tikėtiną prognozuojamą naudą, kurią gaus organizaciją, įgyvendinusi tam tikrą rizikos valdymo techniką (LSD, 2018). Neabejotina, kad rizikos mažinimas organizacijoje yra vienas iš svarbiausių aspektų, leidžiančių minimizuoti kibernetinio saugumo incidentų atsiradimo grėsmę ar įvykusio kibernetinio incidento padarinių mastą, tačiau kartais jis yra ekonomiškai nepagristas ir tuomet gali būti

svarstytinas kitokios rizikos valdymo technikos panaudojimas. Pažymėtina, kad, susiklosčius minėtai situacijai, organizacijos vadovams turi būti pristatytos visos įmanomos alternatyvios rizikos valdymo technikų panaudojimo galimybės, o vadovybė yra atsakinga už sprendimo priėmimą, pasirenkant rizikos valdymo techniką. Rizikos valdymo proceso įgyvendinimo metu viešojo ir privataus sektoriaus organizacijos susiduria su panašiais iššūkiais, tačiau jos siekia skirtingų tikslų, o tai lemia, kad finansinis rodiklis ne visuomet turi būti esminiu aspektu, pasirenkant rizikos valdymo priemones (Coram ir kt., 2006; Ackermann, 2012; ISO, 2018; Patiño, Yoo, 2018);

- *Parengti organizacijos kibernetinio saugumo rizikų valdymo planą,* kuriame būtų aiškiai identifikuoti nustatytų rizikų prioritetai, apibrėžtos kiekvienos iš nustatytų rizikų valdymo priemonės ir būtini veiksmai, kuriuos turi atlikti organizacija, įgyvendindama tas priemones bei numatytas valdymo priemonių įgyvendinimo laikotarpis. Sudarydama identifikuotų rizikų sąrašus ir nustatydama jų prioritetus bei kurdama priemonių įgyvendinimo laiko ašį, organizacija gali pasinaudoti rizikų pavojingumo vertinimo ataskaita bei rizikos valdymo priemonių įgyvendinimo kaštų ir tikėtinos naudos santykio apskaičiavimo metodikomis, tačiau konkrečių priemonių įgyvendinimo sprendimai turi būti tvirtinami organizacijos vadovybės, atsižvelgiant į skiriamus asignavimus. Taip pat organizacija turi atsižvelgti į dabartinius išteklius, skiriamus kibernetiniam saugumui užtikrinti organizacijoje, kadangi kiekvienoje organizacijoje yra naudojamos tam tikros organizacinės ar technologinės kibernetinio saugumo valdymo priemonės. Dažnai naujų ir technologiškai sudėtingesnių sprendimų įgyvendinimas reikalauja didelių finansinių išlaidų, kurių galima išvengti, patobulinus jau dabar naudojamas technologijas ar organizacines tvarkas, o jų įdiegimas organizacijoje iš esmės nedaro įtakos kibernetinio saugumo situacijos pokyčiams (Agrawal ir kt., 2014; Proença ir kt., 2017; ISO, 2018; LSD, 2018);
- *Atlikti kibernetinio saugumo rizikos valdymo plano įgyvendinimo organizacijoje vertinimą*, kuris suteiks galimybę nustatyti, kaip anksčiau minėtų kibernetinio saugumo rizikos valdymo dimensijos priemonių įgyvendinimas veikė rizikos valdymą organizacijoje. Vykdant šios priemonės įgyvendinimą, organizacijoje bus identifikuota egzistuojančių rizikų valdymo pokyčio dinamika, taip pat organizacija turės galimybę įvertinti rizikos valdymo priemonių diegimo efektyvumą bei, esant reikalui, galės koreguoti kibernetinio saugumo rizikų valdymo planą. Pažymėtina, kad įgyvendintų rizikų mažinimo priemonių efektyvumo vertinimas turi būti aiškiai reglamentuotas ir suprantamas, taip pat pritaikytas konkrečios organizacijos veiklai, siekiant išvengti netinkamo vertinimo, kuris gali netinkamai nustatyti rizikos valdymo proceso įgyvendinimą organizacijoje, taip sudarant galimybę netinkamai įvertinti galimas rizikas ir jų sukeliamas grėsmes. Įgyvendindama šią priemonę, organizacija gali pasinaudoti savo turimais vidiniais resursais arba įtraukti į šią veiklą kitą organizaciją ar specialistus, kurie turi pakankamai kompetencijų ir sugebės užtikrinti sklandų šio proceso įgyvendinimą.

Įgyvendinant kibernetinio saugumo rizikos valdymo dimensijos trečiąjį lygmenį organizacijoje, turi būti aiškiai suprantama, kad visos kibernetinio saugumo valdymo modelio dimensijos turi būti pasiekusios antrąjį brandumo lygį, o trečiame lygyje bus vykdoma visa visų dimensijų integracija. Trečiojo kibernetinio saugumo modelio lygmens įgyvendinimas organizacijoje lemia kibernetinio saugumo valdymo proceso virsmą į integruotą organizacijos veiklą, kuri tampa neatsiejama nuo visų kitų veiklos procesų ir nuo kurios priklauso darni visos organizacijos plėtra.

Apibendrinant kibernetinio saugumo valdymo modelio rizikos valdymo dimensiją, būtina pažymėti, kad šios dimensijos priemonių įgyvendinimo tikslas yra siejamas su organizacijos poreikiu ir būtinybe suprasti egzistuojančias ir galimas rizikas, kurios gali veikti organizacijos veiklą. Rizikų, kylančių iš organizacijos vidinės ir išorinės aplinkos, identifikavimas ir suvokimas yra pirmasis žingsnis, suteikiantis organizacijai galimybę imtis priemonių, kurios ateityje gali stipriai sumažinti kibernetinių incidentų tikimybę bei pasirengti tinkamai reaguoti į atsirandančias grėsmes. Organizacija, kuri savo veikloje sugeba tinkamai įgyvendinti rizikos valdymo procesus, laiku koreguoti rizikos valdymo planus bei tinkamai įgyvendinti rizikos valdymo priemones, ilgainiui tampa atsparesnė kibernetinėms grėsmėms bei pažeidžiamumams. Akcentuotina, kad, stebint organizacijos vidinės ir išorinės aplinkos kibernetinio saugumo situacijos pokyčius, suprantant kibernetinių incidentų prigimtį ir grėsmių raidos tendencijas, galima numatyti priemones, kurios ateityje padės išvengti kibernetinių grėsmių arba padės sumažinti galimai įvyksiančių kibernetinių incidentų padarinius.

3.2.7. Kibernetinių incidentų valdymo dimensijos analizė

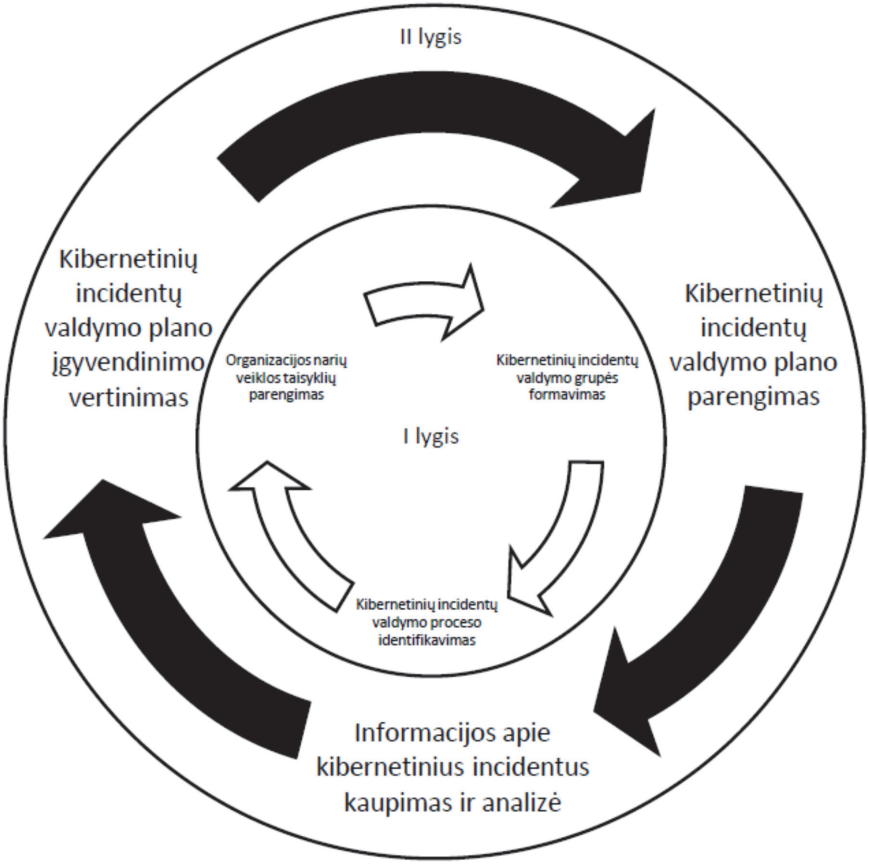
Šiuolaikiniame, technologijomis grindžiamame, pasaulyje egzistuoja daugybė sudėtingų informacinių sistemų. Šias sistemas naudojančios ir valdančios organizacijos nuolatos susiduria su daugybe kibernetinių grėsmių, kurios kasmet tampa vis sudėtingesnės ir įmantresnės. Neatsakingas informacinių sistemų naudotojų elgesys kibernetinėje erdvėje ir su šiais veiksmais susiję kibernetiniai incidentai gali stipriai paveikti organizacijos veiklą ir jos informacinių išteklių naudojimą, o galimai įvyksiantys kibernetiniai išpuoliai prieš organizacijos valdomą kritinę infrastruktūrą gali padidinti chaosą, kurį sukelia saugumo incidentas. Organizacijos techninis personalas, reaguodamas į kibernetinį incidentą ir siekdamas sumažinti organizacijai padarytą žalą bei atstatyti įprastinę organizacijos veiklą, neabejotinai imsis visų įmanomų incidento lokalizavimo ir jo padarinių šalinimo priemonių, tačiau dažnai vykstančio incidento metu organizacijos vadovai reikalauja iš techninio personalo informacijos apie organizacijai padarytus nuostolius, šių nuostolių įtaką organizacijai bei šių nuostolių atsiradimo aplinkybes, taip nesąmoningai galimai komplikuodami situaciją.

Organizacijos ir jos narių gebėjimas tinkamai ir efektyviai reaguoti į kibernetinio saugumo incidentus ne tik suteikia organizacijai galimybę sumažinti galimos kibernetinės atakos sukeltą žalą, bet ir pagreitinti organizacijos įprastinės veiklos atstatymą bei sumažinti kibernetinio incidento sukeltus padarinius. Siekdama įgyvendinti

tinkamus reagavimo į kompiuterinius incidentus organizacinius įpročius, palengvinti techninio personalo darbą ir sumažinti galimus organizacijos nuostolius, organizacija privalo įgyvendinti tam tikrą kibernetinių incidentų valdymo politiką, procedūras ir priemones.

Kibernetinio saugumo incidentų valdymo dimensija, nagrinėjama šioje disertacinio darbo dalyje, kaip jau buvo minėta anksčiau, yra glaudžiai susieta su kibernetinio saugumo valdymo modelio teisinio reguliavimo dimensija. Pažymėtina, kad kibernetinių incidentų valdymas yra labiau susijęs su konkrečių kibernetinio saugumo pažeidžiamumų ir galimai atsirasiančių grėsmių valdymu bei jų prevencija, aprašant konkrečius identifikuotų atsakingų organizacijos narių veiksmus kibernetinių incidentų valdymo srityje, o kibernetinio saugumo valdymo modelio teisinio reglamentavimo dimensijoje yra nagrinėjami ir nustatomi organizacijos narių santykiai su organizacijos vidine ir išorine aplinka, kibernetinio incidento valdymo procese dalyvaujančių organizacijos narių pavaldumo ryšiai bei nurodomos atsakomybės ribos kibernetinių incidentų ir galimų grėsmių atsiradimo ir suvaldymo laikotarpiu. Kibernetinių incidentų valdymo dimensija iš esmės nagrinėja organizacijos galimybę, pasinaudojant administracinėmis saugumo priemonėmis, reglamentuoti bei įgyvendinti kibernetinių saugumo incidentų valdymą, parengiant efektyvius incidentų valdymo planus ir organizacijos narių veiklos taisykles, kurių įgyvendinimas ateityje suteiks organizacijai būtiną gebėjimą laiku identifikuoti ateityje galimai atsirasiančias grėsmes ir, aptikus vykstančią kibernetinę ataką ar įvykusį incidentą, imtis visų reikalingų veiksmų jiems lokalizuoti, sumažinant galimus padarinius arba atkuriant normalią kasdienę organizacijos veiklą bei veiklos procesus.

Kibernetinių incidentų valdymo dimensija grafiškai yra pavaizduojama žemiau esančiame paveiksle (žr. 20 paveikslą).



Šaltinis: *Sudaryta autoriaus*

20 paveikslas. *Kibernetinio saugumo incidentų valdymo dimensija*

Mokslininkai, vyriausybinės organizacijos, kompiuterių saugumo ekspertai ir verslo kompanijų atstovai, kalbėdami apie kibernetinio saugumo incidentų valdymą organizacijoje, neabejoja, kad tai yra viena iš svarbiausių priemonių, siekiant apsaugoti valdomus išteklius. Pažymėtina, kad pasauliniame kibernetinio saugumo kontekste egzistuoja dvejopas požiūris į kibernetinio saugumo incidentų valdymą:

- Kibernetinių incidentų valdymas yra suprantamas kaip *atsakas į kibernetinius incidentus* (*angl. incident response*). Šio požiūrio šalininkai, nagrinėdami kibernetinių incidentų (saugumo incidentų) valdymą, traktuoja jį kaip veiksmų seką, kurių metu organizacija, pasinaudodama tam tikromis technologinėmis priemonėmis ir veiklos taisyklėmis, sugeba efektyviai pasipriešinti vykstančiam kibernetinio saugumo incidentui, jį aptikus, arba atstatyti įprastinių organizacijos veiklos procesų vykdymą bei pašalinti įvykusio incidento padarinius;

- Kibernetinių incidentų valdymas yra suprantamas kaip kibernetinių incidentų tvarkymas (*angl. incident handling*). Šis požiūris į kibernetinio saugumo incidentų valdymą yra traktuojamas kaip procesų ir iš anksto nustatytų procedūrinių veiksmų rinkinys, kuriuo organizacija gali sėkmingai ir veiksmingai pasipriešinti kibernetiniams incidentams ir juos valdyti (NIST, 2012; Johansen, 2017; Petters, 2018; Marine, 2018; Reddy, 2019).

Atkreiptinas dėmesys, kad, šiame disertaciniame darbe nagrinėjant kibernetinio saugumo incidentų valdymo dimensiją, abu anksčiau minėti požiūriai į kibernetinio saugumo incidentų valdymą nebus atskiriami vienas nuo kito, o pats kibernetinių incidentų valdymas darbe yra suprantamas kaip vientisas dalykas, savyje sujungiantis procesus, taisykles ir žinias bei gebėjimus, kurie yra būdingi organizacijai, atsižvelgiant į jos turimus išteklius. Kitaip tariant, kibernetinių saugumo incidentų tvarkymas ir atsakas į kibernetinius saugumo incidentus šiame disertaciniame darbe yra suprantamas kaip bendras reiškinys. Toks požiūris į kibernetinių incidentų valdymą suteiks organizacijai galimybę geriausiai įgyvendinti šią modelio dimensiją. Mokslininkai ir kibernetinio saugumo organizacijos pažymi, kad atsako į incidentus ir saugumo incidentų tvarkymo funkcijų sujungimas organizacijoje suteikia galimybę išvengti netinkamo kibernetinių incidentų valdymo, eliminuojant netinkamo informacijos srautų judėjimo, pavaldumo, bendradarbiavimo tarp atsakingų organizacijos narių ir technologinių žinių stokos problemas (NIST, 2012; Johansen, 2017; Schreck, 2018; Reddy, 2019).

Toliau esančioje lentelėje (žr. 14 lentelę) yra pateikiamos kibernetinio saugumo valdymo modelio incidentų valdymo dimensijos priemonės, kurių įgyvendinimas organizacijoje suteiks jai galimybę efektyviai valdyti galimai įvyksiančius, vykstančius ar įvykusius kibernetinio saugumo incidentus, taip pat laiku ir, tikėtina, minimaliomis sąnaudomis šalinti jų padarinius.

14 lentelė. *Kibernetinio saugumo incidentų valdymo dimensijos įgyvendinimo priemonės*

Kibernetinio saugumo incidentų valdymo dimensija		
1 lygis	**2 lygis**	**3 lygis**
Suformuoti organizacijoje kibernetinių incidentų valdymo grupę.	Parengti kibernetinio saugumo incidentų valdymo planą organizacijoje.	Kibernetinio saugumo incidentų valdymo dimensijos integravimas ir sujungimas su kitomis kibernetinio saugumo valdymo modelio dimensijomis.
Nustatyti kibernetinio saugumo incidentų valdymo proceso ypatumus organizacijoje.	Kaupti ir analizuoti informaciją apie kibernetinio saugumo incidentus.	
Parengti pradines organizacijos narių veiklos instrukcijas, įvykus kibernetiniam incidentui.	Atlikti kibernetinio saugumo incidentų valdymo plano įgyvendinimo vertinimą.	

Šaltinis: *Sudaryta autoriaus*

Pasaulio mokslininkų, kibernetinio saugumo ekspertų ir kibernetinį saugumą užtikrinančių institucijų manymu, organizacijoje yra būtina įgyvendinti kibernetinių incidentų valdymo procesą, o pats kibernetinių incidentų valdymas, kruopščiai apibrėžiantis visas incidentų tvarkymo ir reagavimo į juos taisykles ir procesus, neabejotinai yra laikomas viena iš svarbiausių kibernetinių grėsmių vengimo ir prevencijos priemonių, suteikiančių galimybę laiku ir tinkamomis priemonėmis reaguoti į vykstantį incidentą, mažinti jo padarinius arba atstatyti organizacijos įprastą veiklą po įvykusios kibernetinės atakos (Shultz, Shumway, 2001; Freiling, Schwittay, 2007; NIST, 2012; Johansen, 2017; Schreck, 2018; Reddy, 2019).

Siekiant sklandaus kibernetinio saugumo incidentų valdymo dimensijos įgyvendinimo organizacijoje, pirmiausiai turi būti įgyvendintos toliau išvardytos pirmojo lygio priemonės:

- *Suformuoti organizacijoje kibernetinių incidentų valdymo grupę,* į kurią bus paskirti skirtingų organizacijos struktūrinių vienetų (departamentų, skyrių ir kt.) atstovai. Šios grupės sudarymas organizacijoje bei skirtingų organizacijos veiklos sričių atstovų įtraukimas į šios grupės darbą ir vykdomas užduotis leis organizacijai aiškiai identifikuoti labiausiai organizacijai priimtiną incidentų valdymo proceso organizavimą bei užtikrins, kad kibernetinių incidentų valdymas bus vykdomas, atsižvelgiant į organizacijos poreikius bei turimus išteklius ir galimybes. Rekomenduojama į kibernetinio saugumo valdymo grupę paskirti techninius specialistus, kurie turi praktinių žinių informacinių ir telekomunikacinių ryšių srityje bei žino, kokiomis techninėmis priemonėmis ir kokiais metodais yra vykdomas kibernetinių incidentų aptikimas ir jų sukeltų padarinių šalinimas; finansinius išteklius valdančio ir kontroliuojančio padalinio atstovus, kurie galėtų identifikuoti galimus finansinius organizacijos pajėgumus, kurie bus reikalingi incidentų valdymo procesui įgyvendinti; personalo valdymo padalinio atstovus; vidaus saugumo užtikrinimo padalinio atstovus; teisininkus ir kt. Sudarius tinkamą kibernetinių incidentų valdymo grupę bei užtikrinus jai aukščiausios organizacijos vadovybės palaikymą, galima tikėtis, kad įgyvendinamas incidentų valdymo procesas užtikrins laiku ir tinkamą organizacijos atsaką, įvykus kibernetiniam incidentui;
- Būtina *nustatyti kibernetinio saugumo incidentų valdymo proceso ypatumus organizacijoje*. Šios priemonės įgyvendinimas suteiks organizacijai žinių apie dabartiniu metu egzistuojantį kibernetinių incidentų valdymo procesą, kuris neabejotinai vyksta organizacijoje, nors ir nėra aiškiai identifikuotas ar teisiškai reglamentuotas. Atkreiptinas dėmesys, kad labai dažnai kibernetinių incidentų valdymas organizacijoje egzistuoja kaip tam tikra organizacinės (institucinės) atminties funkcija, o darbuotojai vykdo kibernetinių incidentų valdymą, pasinaudodami savo žiniomis, organizacijos įpročiais bei nusistovėjusiomis „nerašytomis taisyklėmis“. Nustatant incidentų valdymo ypatumus organizacijoje, būtina atsižvelgti į visas galimybes ir apribojimus, kurie gali daryti įtaką sklandžiam šio organizacijos vykdomo proceso įgyvendinimui arba jį paspartinti. Galima paminėti, kad viena iš galimybių yra siejama su organizacijoje egzistuojančio, teisiškai

nereglamentuoto incidentų valdymo modelio panaudojimu ateityje. Įgyvendindama šią priemonę, anksčiau aprašyta kibernetinio saugumo valdymo grupė turi aiškiai identifikuoti egzistuojančio incidentų valdymo proceso pokyčius, jo suderinamumą su ateityje įgyvendinamu valdymu ir, esant galimybei, panaudoti dabartinius incidentų valdymo metodus ateityje, tokiu būdų sumažinant pokyčių kiekį personalui, dalyvaujančiam incidentų aptikimo ir šalinimo procese;

- *Parengti pradines organizacijos narių veiklos instrukcijas*, kurios gali padėti identifikuoti ir aptikti kibernetinius incidentus organizacijoje. Šios priemonės įgyvendinimo metu organizacijoje turi būti parengtos minimalios instrukcijos organizacijos nariams, kurie naudoja organizacijos kompiuterinius išteklius kasdienėje savo veikloje. Pažymėtina, kad šioje priemonėje minimos instrukcijos yra skirtos ne techniniam organizacijos personalui, vykdančiam informacinių ir ryšių technologijų sistemų priežiūrą (informacinių technologijų departamentui ar skyriui), o darbuotojams, kurie nėra susiję su techninės ir programinės įrangos valdymu ir jos veikimo užtikrinimu organizacijoje. Šių minimalių instrukcijų parengimas, personalo supažindinimas su šiomis instrukcijomis leis organizacijai net pirmame kibernetinio saugumo incidentų valdymo modelio dimensijos lygmenyje stipriai pagerinti kibernetinio saugumo incidentų valdymą, kadangi organizacijos nariai bus informuoti apie galimus kibernetinio saugumo incidentus bei atakas ir galės jas atpažinti. Būtent incidentų požymių identifikavimas, organizacijos personalo informavimas apie grėsmes ir aiškių veiksmų eigos nustatymo, aptikus incidentą, suderinimas organizacijoje gali labai padidinti organizacijos kibernetinio saugumo lygį. Mokslininkai ir kibernetinio saugumo ekspertai pažymi, kad organizacijos personalo žinios, susijusios su būtinais veiksmais, kurių turi imtis darbuotojas, aptikęs galimai vykstantį kibernetinį incidentą ar kibernetinės atakos požymius, vis dar yra nepakankamos ir dažniausiai šių žinių stoka veikia organizacijos kibernetinį saugumą ir išlieka viena iš svarbiausių kibernetinių incidentų priežasčių (Knapp ir kt., 2006; Harrison, White, 2011; Agrawal ir kt., 2014; Alotaibi ir kt., 2016; Vadiveloo ir kt., 2016; Dunkelberg, 2017).

Organizacijai, sėkmingai įgyvendinus kibernetinio saugumo valdymo modelio incidentų valdymo dimensijos pirmojo lygmens priemones, būtina imtis antrajame dimensijos lygyje esančių priemonių įgyvendinimo:

- *Parengti kibernetinio saugumo incidentų valdymo planą organizacijoje*, kuriame bus apibrėžti visos organizacijos ir jos narių veiksmai, kurių organizacija privalo laikytis kibernetinio incidento metu, taip pat aprašyti su kibernetinio incidento valdymu susiję procesai, kurie turi būti įgyvendinti organizacijoje, siekiant padidinti organizacijos atsparumą galimoms kibernetinėms grėsmėms ir vykstantiems incidentams. Rengiant kibernetinio saugumo incidentų valdymo planą organizacijoje, būtinas pačios organizacijos suvokimas, kad kiekvienas kibernetinis incidentas turi tam tikrą gyvavimo ciklą. Tinkamas organizacijos pasiruošimas kibernetinio incidento gyvavimo ciklo etapuose vykstantiems procesams užtikrina sėkmingą kibernetinio incidento suvaldymą, taip pat padidina organizacijos

atsparumą ateities kibernetinėms grėsmėms. Pažymėtina, kad mokslininkai ir kibernetinio saugumo organizacijos kibernetinio incidento pradžią organizacijoje sieja su laikotarpiu, kai organizacija pirmą kartą sužino apie veiklą, įvykį arba įvykių seką, turinčią kenkėjiškų veiksmų, nukreiptų prieš organizacijos valdomus išteklius, požymių (ITU, 2015; Johansen, 2017; Schreck, 2018). Informaciją apie grėsmę organizacijai gali būti pateikta skirtingais būdais – iš automatinės perspėjimo sistemos, taip pat iš išorinės ar vidinės organizacijos aplinkos arba kitais būdais. Bet kurio atveju organizacija privalo imtis veiksmų ir reaguoti į informaciją apie galimai įvyksiantį kibernetinį incidentą, o pats reagavimas ir incidento suvaldymas turi būti vykdomas šešiais, vienas po kito sekančiais etapais, kurie yra išvardyti toliau:

- *Pasirengimas incidentui*, kuris suteikia organizacijai galimybę tinkamai planuoti turimų išteklių panaudojimą ir veiksmus incidento metu. Tinkamas pasirengimo incidentui veiksmų įgyvendinimas užtikrina tolimesnių veiksmų, sprendžiant kibernetinio saugumo incidentą, suderinamumą ir efektyvumą. Organizacijai tinkamai nepasirengus, atsiranda rizika, kad tolimesni organizacijos veiksmai, sprendžiant kibernetinio saugumo incidentą, bus vykdomi chaotiškai, kas, savo ruožtu, tik padidins incidento sukeltą žalą bei sudarys prielaidas netinkamam išteklių panaudojimui, šalinant kibernetinį incidentą ir jo sukeltus padarinius. Pažymėtina, kad šio etapo įgyvendinimo metu turi būti parengtos aiškios taisyklės (reglamentuoti procesai ir procedūros), kurios bus naudojamos organizacijoje, kovojant su kibernetinio incidento sukeltomis grėsmėmis, tai pat sudaryti organizacijos narių (personalo), dalyvaujančių incidento šalinime, sąrašai, nusakantys jų vykdomas funkcijas kibernetinio incidento metu. Įgyvendinus anksčiau minėtus dalykus, būtina užtikrinti tinkamą organizacijos narių (reagavimo į incidentus personalo) apmokymą, kuris apimtų ne tik incidento valdymo metu vykstančius procesus ir procedūras, bet ir visų technologinių priemonių, reikalingų kibernetinio incidento šalinimo metu, panaudojimą. Galiausiai, siekiant įsitikinti, kad organizacija yra pajėgi tinkamai reaguoti į kibernetinius incidentus ir gali su jais kovoti, būtina vykdyti reguliarias kibernetinių incidentų valdymo ir jų sukeltų padarinių šalinimo pratybas;
- *Incidento aptikimas* – etapas, kurio metu organizacija, pasinaudodama visais jai prieinamais informacijos šaltiniais ir informacijos gavimo kanalais bei technologinėmis kibernetinių grėsmių aptikimo priemonėmis, gali identifikuoti prieš ją nukreiptus veiksmus, turinčius kibernetinių incidentų ar kibernetinių atakų požymių. Pažymėtina, kad kibernetinio incidento aptikimas yra labai sudėtingas procesas, kurį lemia keletas svarbių faktorių: organizacijos dydis, valdomų išteklių kiekis (technologinės ir programinės įrangos gausa), organizacijos geografinis išsidėstymas (atstovybių gausa) ir kt. Informacija apie galimą incidentą gali pasiekti organizaciją skirtingais kanalais: iš organizacijos naudojamų programinės įrangos spragų aptikimo sistemų, duomenų perdavimo tinklų sensorių, įsibrovimų aptikimo sistemų, ryšio paslaugų teikėjų, teisėsaugos institucijų, organizacijos narių ir kt. Atsižvelgiant į organizacijos dydį ir kitus faktorius, kasdien

pranešimų apie galimas kibernetines grėsmes gali būti šimtai tūkstančių, tačiau kiekvienas iš šių pranešimų turi būti apdorojamas ir traktuojamas kaip kibernetinis incidentas. Būtent toks požiūris į kibernetinių incidentų aptikimą ilgainiui leis organizacijos nariams (kibernetinio saugumo analitikams) nustatyti nepavojingus ir netikrus (*angl. false-positive*) saugumo įvykius ir palengvins ateityje įvyksiančių kibernetinių incidentų identifikavimą bei minimizuos kibernetinio incidento neaptikimo grėsmę;

- *Incidento analizės* etapas, kurio metu organizacijos nariai nagrinėja kibernetinio saugumo incidentą, siekdami aiškiai identifikuoti galimo incidento įtaką organizacijos valdomiems ištekliams. Šiame etape yra renkama informacija apie galimo kibernetinio incidento įtaką organizacijos informacinėms sistemoms, ryšių ir telekomunikaciniams tinklams, technologiniams ar programiniams produktams, naudojamiems organizacijos veikloje. Incidento analizės etapo metu organizacija gali naudoti ne tik savo turimus išteklius, bet ir, esant reikalui, pasitelkti kitas kompetentingas šalis. Atsižvelgiant į kibernetinio saugumo incidento tipą, saugumo spragos išnaudojimo laikotarpį, organizacijos valdomų informacinių išteklių dydį, darbuotojų kompetentingumą ir dar daugelį kitų faktorių, incidento analizės etapas gali trukti nuo kelių valandų iki kelių dienų. Pagrindinis šio etapo tikslas yra siejamas su organizacijos galimybe, pasinaudojant technologinio kibernetinio saugumo priemonėmis ir turima informacija apie incidentą bei ją sujungus su atitinkamomis kompetentingų organizacijos narių žiniomis, identifikuoti kibernetinio incidento priežastį, eigą, paplitimą, poveikį organizacijai ir jos valdomoms informacinėms sistemoms ir kt. Pažymėtina, kad būtent šiame etape atlikti veiksmai aiškiai identifikuoja kibernetinio incidento sukėlėjo veiksmus laikotarpyje nuo incidento atsiradimo iki jo aptikimo, gali nurodyti grėsmės sukėlėjo siektinus tikslus ir parodyti organizacijai veiksmus, kurių būtina imtis, siekiant sustabdyti kibernetinės grėsmės plitimą organizacijoje;
- *Incidento lokalizavimo* etapas, skirtas organizacijos veiksmams, kurie yra nukreipti į aiškiai identifikuoto kibernetinio saugumo incidento plitimo sustabdymą ir izoliavimą. Incidento suvokimas, jo veikimo algoritmo supratimas bei aiškus kibernetinio saugumo incidento paveiktų organizacijos valdomų išteklių ir poveikio dydžio identifikavimas, atliktas incidento analizės etape, sudaro prielaidas efektyviai lokalizuoti kibernetinį incidentą ir sustabdyti jo plitimą. Incidento lokalizavimo metu organizacija turi imtis visų jai prieinamų kibernetinio saugumo valdymo priemonių, apribojant grėsmės sukėlėjų galimybes toliau kompromituoti organizacijos valdomus informacinius išteklius ir sistemas bei didinti kibernetinio incidento paveiktų sistemų kiekį. Vykdydama kibernetinio incidento lokalizavimą, organizacija, siekdama užkirsti kibernetinės grėsmės tolimesnę plėtrą, gali naudotis ne tik technologinėmis kibernetinio saugumo priemonėmis (pvz., ugniasienėmis, maršrutizatorių nustatymais ir kt.), bet ir imtis fizinės prieigos prie informacinių išteklių apribojimo (pvz., atjungiant kibernetinės atakos metu paveiktas darbo ar tarnybines stotis nuo organizacijos duomenų perdavimo tinklo). Organizacijos nariai, dalyvaujantys kibernetinio incidento valdymo

procese, turi patys, atsižvelgdami į susiklosčiusią situaciją ir turimą patirtį bei žinias, nuspręsti, kokie konkretūs veiksmai ir kokių priemonių panaudojimas bus efektyviausias konkretaus kibernetinio incidento metu, bei nedelsdami imtis šių priemonių. Pažymėtina, kad incidento lokalizavimas, kaip ir kai kurie kiti reagavimo į kibernetinius incidentus etapai, gali būti vykdomi ne tik vykstančio kibernetinio incidento metu, bet ir prieš jam įvykstant, kai organizacija imasi prevencinių veiksmų, siekdama sumažinti žalą nuo galimai ateityje atsirasiančio kibernetinio incidento;

- *Incidento šalinimas ir normalios organizacijos veiklos atstatymo* etapas yra skirtas visiškam kibernetinį incidentą sukėlusiai grėsmei iš organizacijos valdomų informacinių išteklių pašalinti, taip pat įprastų organizacijos veiklos procesams ir darbui atstatyti. Pradinis šio etapo tikslas yra eliminuoti kibernetinio incidento sukėlėjo galimybes sėkmingai tęsti kibernetinę ataką prieš organizaciją bei daryti įtaką kasdienei organizacijos veiklai po kibernetinio incidento aptikimo, analizės ir lokalizavimo. Organizacijai, siekiančiai normalizuoti savo veiklos procesus, šalinančiai technologinės ir programinės įrangos sutrikimus, atsiradusius dėl kibernetinio incidento, būtina atlikti visų paveiktų informacinių išteklių, identifikuotų incidento analizės metu, atstatymą: iš naujo įdiegti darbo ir tarnybinių stočių operacines sistemas ir taikomąją programinę įrangą, panaikinti nenaudojamas vartotojų ir technologinių sistemų administruojančio personalo prisijungimo prie informacinių išteklių sąskaitas, pakeisti (atnaujinti) tinklo valdymo įrenginių aparatinės dalies valdymo programinę įrangą ir nustatymus pagal gamintojo pateikiamus vėliausius atnaujinimus, atlikti ugniasienių ir kitų tinklo saugumo įrenginių nustatymų peržiūrą ir kt. Pažymėtina, kad organizacijai, kuri įtaria, kad tam tikra jos valdoma informacinė infrastruktūra yra paveikta kibernetinio incidento metu, bet incidento poveikis nėra aiškiai identifikuotas arba nėra žinomas poveikio dydis, rekomenduojama atlikti galimų atakos pasekmių šalinimą ir šioje informacinėje infrastruktūroje, siekiant maksimaliai sumažinti nepastebėtos grėsmės poveikį organizacijai ateityje. Atkūrimo po kibernetinio incidento veikla organizacijoje yra labai panaši į tą, kuri gali būti nustatyta organizacijos verslo tęstinumo ar atkūrimo po nelaimių planuose, o atlikus visus būtinus technologinius veiksmus organizacijos valdomoje informacinėje infrastruktūroje, turi būti atliktas pažeidžiamumų nuskaitymas, parodantis, kad organizacijos valdoma infrastruktūra yra saugi, o pažeidžiamumai, galintys veikti organizacijos procesus, buvo pašalinti;
- *Incidento šalinimo veiksmų analizės* etapas, kuriame yra vykdoma visos organizacijos ir jos narių bei kitų į incidento suvaldymą įtrauktų suinteresuotų asmenų veiksmų, kurių buvo imtasi, reaguojant į kibernetinio saugumo incidentą, jį suvaldant ir šalinant jo pasekmes, analizė. Šio etapo metu būtina aiškiai identifikuoti, kokios naudojamos priemonės ir organizacijos veiklos procesai prisidėjo prie efektyvaus kibernetinio incidento suvaldymo, o svarbiausia, išsiaiškinti, kokios priemonės neveikė ir kokios šių priemonių sutrikimų priežastys. Šio etapo metu organizacija turi galimybę aiškiai identifikuoti organizacijos narių

incidento metu atliktus veiksmus ir vykdytas konkrečias užduotis, kurie turėjo teigiamą arba neigiamą poveikį reagavimo į incidentą rezultatams. Šiame etape parengiama kibernetinio saugumo incidento suvaldymo ataskaita, išsamiai parodanti aiškią įvykių eigą, sutelkiant dėmesį į pagrindinę priežastį, dėl kurios įvyko incidentas, jei ji buvo nustatyta. Šios ataskaitos rengėjai turėtų suvokti, kad parengtos ataskaitos medžiaga turės būti pristatoma organizacijos nariams bei aukščiausios grandies vadovams, todėl būtina greta technologinių aspektų pateikti ir įvykių aprašymą, paaiškinant technologinį žargoną ir sąvokas. Parengus incidento šalinimo veiksmų analizės ataskaitą, turi būti identifikuotos galimos įvykusio incidento šalinimo veiksmų spragos, o organizacija turi atnaujinti procesus, susijusius su reagavimu į incidentus, taip pat pateikti informaciją į duomenų bazę, kurioje kaupiama informacija apie organizacijoje įvykusius incidentus, kadangi tai padeda ateityje efektyviau reaguoti į galimus incidentus, atsižvelgiant į „išmoktas pamokas“.

- *Kaupti ir analizuoti informaciją apie kibernetinio saugumo incidentus*, siekiant suteikti organizacijai galimybę tinkamai pasiruošti ateityje įvyksiantiems incidentams bei sudaryti sąlygas tinkamai reaguoti į grėsmes, atsirandančias kibernetinėje erdvėje. Įgyvendindama šią priemonę, organizacija turi sukurti kibernetinių incidentų valdymo („išmoktų pamokų“) duomenų bazę, į kurią bus įtraukiami duomenys, susiję su organizacijoje aptiktų kibernetinių incidentų valdymu ir jų sukeltų padarinių šalinimu, taip pat informacija apie kibernetines grėsmes, gaunama iš organizacijos išorinės aplinkos. Tokios duomenų bazės sukūrimas, kaupiamų duomenų atnaujinimas laiku ir turimų duomenų analizės procesas suteiks organizacijai pranašumą prieš kibernetinių incidentų sukėlėjus. Organizacijos valdoma informacija apie aktualias kibernetines grėsmes, pasaulines kibernetinių incidentų ir atakų plėtros tendencijas, kibernetinių išpuolių realizavimo mechanizmus ir metodus neabejotinai prisidės prie organizacijos galimybės tinkamai reaguoti į grėsmes, pasiruošti ateityje galimai įvyksiantiems kibernetinio saugumo incidentams ir užtikrinti sklandų kibernetinių incidentų valdymo proceso įgyvendinimą organizacijoje. Kai kurios pasaulio valstybės, siekdamos užtikrinti kibernetinį saugumą, kuria duomenų bazes, į kurias yra sudedama visa informacija apie kibernetinius incidentus, įvykusius viešojo sektoriaus organizacijų infrastruktūroje. Tokių duomenų bazių informacija yra viešai prieinama ir be jokių apribojimų ar papildomų mokesčių gali būti naudojama bet kokios organizacijos kibernetinio saugumo valdymo procese, siekiant maksimaliai sumažinti kibernetinio saugumo informacinio vakuumo atsiradimą organizacijoje, taip pat užtikrinti tinkamą reagavimą į žinomas grėsmes ir efektyvų kibernetinių incidentų valdymą.
- *Kibernetinio saugumo incidentų valdymo plano* įgyvendinimo *vertinimas ir koregavimas*, kurio metu organizacija galės nustatyti, ar visos plane numatytos priemonės buvo tinkamai įgyvendintos ir kaip tai paveikė kibernetinių saugumo incidentų valdymą organizacijoje. Pažymėtina, kad šios priemonės įgyvendinimas taip pat suteikia organizacijai galimybę aiškiai identifikuoti incidentų valdymo

proceso trūkumus ir juos pašalinti, atliekant plano koregavimą. Šios dimensijos priemonės įgyvendinimas organizacijos kibernetinio saugumo incidentų valdymo procese taip pat yra priklausomas nuo pasaulinių kibernetinių grėsmių raidos tendencijų, taip pat ir nuo pačios organizacijos galimybės pasinaudoti jai prieinamais duomenimis apie kibernetinio saugumo situaciją vidinėje ir išorinėje aplinkoje. Atsižvelgdama į šiuos faktorius, organizacija turi ne tik periodiškai atlikti plano vertinimą, bet ir tuo pačiu metu koreguoti organizacijos kibernetinių incidentų valdymo procesą, siekdama maksimalaus jo efektyvumo, kadangi, kaip jau buvo minėta anksčiau, kibernetinis saugumas yra labai dinamiškas ir greitai besikeičiantis dalykas, reikalaujantis pastovaus dėmesio. Būtent toks požiūris į kibernetinį saugumą užtikriną, kad visos priemonės, naudojamos kibernetinio saugumo valdymo procese, bus maksimaliai efektyvios, o organizacijos valdomi informaciniai ištekliai išliks saugūs ir, bent jau teoriškai, nepažeidžiami.

Įgyvendinus kibernetinio saugumo incidentų valdymo dimensijos pirmojo ir antrojo lygio priemones bei visoms kitoms kibernetinio saugumo valdymo modelio dimensijoms pasiekus antrąjį lygmenį, turi būti atliekama visų modelio dimensijų tarpusavio sintezė, siekiant užtikrinti visišką kibernetinio saugumo valdymo kompleksiškumą organizacijoje.

Apibendrinant būtina pažymėti, kad kibernetinio saugumo valdymo modelio incidentų valdymo dimensijos priemonių įgyvendinimas labiausiai susijęs su organizacijos poreikiu ir būtinybe gebėti laiku bei maksimaliai efektyviai valdyti kibernetinius incidentus, siekiant sumažinti galimų kibernetinių atakų sukeltą žalą, bei minimizuoti incidentų įtaką organizacijos veiklos procesams. Kiekviena organizacija anksčiau ar vėliau susidurs su kibernetiniu incidentu savo valdomuose ištekliuose, tačiau labai tikėtina, kad laiku ir kruopštus pasiruošimas tam „susidūrimui“ gali sumažinti organizacijos nuostolius bei suteikti galimybę imtis tinkamų priemonių kibernetiniam incidentui suvaldyti.

3.2.8. Veiklos efektyvumo vertinimo sistemos analizė

Kaip jau buvo išnagrinėta anksčiau, kibernetinio saugumo valdymo modelis yra sudarytas iš šešių skirtingų dimensijų, kurios nagrinėja skirtingas kibernetinio saugumo įgyvendinimo sritis, tačiau visos modelio dimensijos turi vieną bendrą atributą (požymį). Kibernetinio saugumo valdymo modelio įgyvendinimas yra neįmanomas be veiklos efektyvumo vertinimo sistemos.

Veiklos efektyvumo vertinimo sistema yra neatskiriama kiekvienos organizacijos valdymo sistemos dalis, kuri suteikia organizacijos nariams ir vadovams galimybę atlikti organizacijos, organizacijos narių ir organizacijoje vykstančių procesų įvertinimą, taip pat įgalina organizacijos struktūrinių padalinių tarpusavio bendradarbiavimą. Ši sistema suteikia organizacijai galimybę išmatuoti savo vykdomos veiklos efektyvumą, nustatyti rezultatų pasiekimo lygį, vykdyti organizacijos pokyčius, atlikti laiku ir būtinas organizacijos veiklos korekcijas, informuoti visus organizacijos narius apie jų vykdomos veiklos rezultatus ir taip pat kontroliuoti organizacijos strategijos įgyvendinimą (Bitici ir kt., 1997; Micheli, Manzoni, 2010; Yadav, Sagar, 2013; Striteska, Jelinkova, 2014).

Pasaulio mokslininkai yra nagrinėję veiklos vertinimo sistemas ir jų panaudojimą efektyvumo vertinimo procese bei pateikę pasauliui įvairių siūlymų, susijusių su veiklos efektyvumo vertinimo sistemos sukūrimu organizacijose (Neely ir kt., 1995; Manoochehri, 1999; Kennerley, Neely, 2002; Micheli, Manzoni, 2010; Gomes ir Yasin, 2011; Striteska, Spickova, 2012; Franco-Santosa ir kt., 2012; Striteska, Jelinkova, 2014), tačiau ne visus mokslininkų pasiūlymus galima taikyti kiekvienoje organizacijoje. Siūlymų tinkamumas yra glaudžiai susietas su organizacijos veiklos sritimi, valdymu, vykdomais veiklos procesais ir kt.

Diegiant kibernetinio saugumo valdymo modelį organizacijoje, reikia aiškiai suprasti, kad veiklos vertinimas taip pat yra būtinas, o pati veiklos vertinimo sistema turi atitikti tam tikrus kriterijus. Atsižvelgiant į pasaulio mokslininkų siūlymus, galima teigti, kad, diegiant kibernetinio saugumo valdymo modelio veiklos efektyvumo vertinimo sistemą, ši sistema turi:

- *būti paprasta ir lengvai panaudojama* (pritaikoma) organizacijos veikloje, kadangi paprastumas (suprantamumas) suteikia galimybę išvengti veiklos vertinimo sistemos panaudojimo klaidų ir netikslaus organizacijos pažangos įvertinimo;
- *aiškiai identifikuoti* (nusakyti) *sistemos panaudojimo tikslą*, kad kiekvienas organizacijos narys suprastų, dėl kokios priežasties yra vykdomas veiklos efektyvumo vertinimas;
- *pateikti organizacijai greitą rezultatą* (grįžtamąjį ryšį), kurio įvertinimas organizacijoje suteiktų galimybes koreguoti visos organizacijos arba jos narių veiklą;
- *apimti visus organizacijos elementus* (finansinius ir nefinansinius veiklos procesus, kokybinius ir kiekybinius vertinimo rodiklius, vidaus ir išorės veiklos procesus), kadangi tik kompleksinis organizacijos veiklos efektyvumo vertinimas suteikia galimybe nustatyti konkrečių sričių korekcijų poreikį, bei greitai ir efektyviai koreguoti organizacijos ar jos narių veiklą;
- *būti susijusi su organizacijos veiklos tobulinimu*, o ne tik su organizacijos veiklos stebėjimu, kadangi tik neefektyviai veikiančių sričių tobulinimas, aktyvūs veiksmai bei pokyčiai, gali padidinti organizacijos efektyvumą;
- *sustiprinti organizacijos strategiją*, pateikiant organizacijai informaciją apie būtinas veiklos korekcijas;
- *būti vienareikšmiškai susieta su organizacijos nusistatytais tikslais*, kadangi organizacijos veiklos efektyvumas turi būti tuo pat metu matuojamas, atsižvelgiant ir į ilgalaikius, ir į trumpalaikius tikslus;
- *būti integruota organizacijos struktūroje* (horizontalus ir vertikalus integravimas), kad būtų įmanoma įvertinti visų organizacijos sluoksnių efektyvumą bei nustatyti, kokiame organizacijos lygmenyje yra būtinos veiklos procesų korekcijos;
- *būti suderinta su darbuotojų veiklos vertinimo ir motyvavimo sistemomis,* kadangi efektyvią veiklą vykdantys organizacijos nariai, gerina pačios organizacijos veiklą ir spartina jos veiklos procesus, prisideda prie organizacijos tikslų įgyvendinimo pagreitinimo. Tokia organizacijos narių veikla ir pavyzdys gali stimuliuoti kitų organizacijos narių norą aktyviau dalyvauti organizacijos veikloje;

- *padėti identifikuoti ir tobulinti neefektyvius procesus*, nustatant trūkumus, kurių pašalinimas gali efektyvinti organizacijos veiklą ir joje vykstančius procesus;
- *suteikti organizacijai galimybę* greitai ir efektyviai *mokytis* ir efektyviai keisti savo veiklos strategiją, atsiradus aplinkos pokyčiams arba numatant greitą tokių veiklos pokyčių atsiradimą. Kitais žodžiais tariant, veiklos efektyvumo vertinimo sistemos paskirtis yra ne tik dabartinės situacijos įvertinimas, bet ir galimų pokyčių ateityje prognozė;
- *vertinti ne konkrečių organizacijos narių* (individų) *veiklą*, *bet* labiau koncentruotis į tam tikrų *skyrių* (darbo grupių, struktūrinių padalinių) *veiklos įvertinimą*, nes tik taip galima identifikuoti ne smulkias individo veiklos problemas, o paties organizacijos veiklos proceso trūkumus ir ribotumus, kurie dažniausiai nepriklauso nuo jos vykdančio individo asmeninių savybių;
- *nustatyti aiškias matavimo skales* kiekybiniams ir kokybiniams vertinimo tikslų rodikliams, kad veiklos vertinimo metu vertintojai negalėtų interpretuoti, iškraipyti vertinimo tikslumą. Nustatant vertinimo skales, rekomenduojama kiekybinius kriterijus matuoti skaitine išraiška, o kokybiniams kriterijams vertinti naudoti vienodas skales;
- *turi būti nuolat vertinama ir tobulinama*, kadangi tik nuolatinis vertinimo ir pritaikymo procesas, atsižvelgiant į besikeičiančias vidaus ir išorės aplinkas, globalizacijos aspektus bei organizacijos evoliuciją, gali leisti vertinimo sistemai išlikti aktualia, kas, savo ruožtu, leis ir pačiai organizacijai tobulėti ir vystytis.

Organizacijos, planuojančios įsidiegti veiklos efektyvumo vertinimo sistemą, turi ne tik įvertinti būsimos sistemos komponentus ir anksčiau aprašytų reikalavimų tinkamumą savo kuriamai sistemai, bet ir nuspręsti, kokius iš šių reikalavimų įgyvendinti, diegiant vertinimo sistemą. Taip pat turi būti aiškiai suprantama, kad kiekvienu atveju organizacijos kuriama veiklos efektyvumo vertinimo sistema turi būti pritaikyta konkrečios organizacijos veiklos sričiai. Diegiant ir naudojant organizacijos veiklos efektyvumo vertinimo sistemą, būtina:

- aiškiai identifikuoti organizacijos misiją;
- pasinaudojant organizacijos identifikuota misija, nustatyti ilgalaikius ir trumpalaikius strateginius tikslus;
- identifikuoti kiekvienos organizacijos vykdomos veiklos funkcinės srities svarbą, siekiant numatytų ilgalaikių ir trumpalaikių tikslų įgyvendinimo;
- identifikuoti organizacijos dabartinę situaciją bei nustatyti pažangos vertinimo kriterijus, matavimo skales ir vertinimo periodiškumą, suderinti šiuos aspektus su organizacijos vadovybe;
- iškomunikuoti organizacijos misiją, strateginius tikslus ir veiklos vertinimo proceso sąlygas visoje organizacijoje;
- parengti organizacijos veiklos vertinimo kriterijus, atsižvelgiant į kiekvienos funkcinės srities specifiką, bei nustatyti konkretesnius (siauresnius) veiklos efektyvumo vertinimo kriterijus;
- užtikrinti specifinių sričių vertinimo kriterijų atitikimą globaliems vertinimo kriterijams bei strateginiams tikslams;

- užtikrinti veiklos vertinimo rezultatų suderinamumą tarp visų organizacijos funkcinių sričių;
- naudoti parengtą vertinimo sistemą, siekiant patobulinti organizacijos veiklą, identifikuoti problemines organizacijos veiklos sritis, pagelbėti organizacijai, atsinaujinant ilgalaikius ir trumpalaikius tikslus, koreguojant strategiją, bei įvertinti organizacijos pokyčius po organizacijos veiklos pokyčių ir galimų transformacijų;
- periodiškai atlikti jau naudojamos sistemos vertinimą ir galimas korekcijas tam, kad sistema visiškai atitiktų šiuolaikines organizaciją supančios aplinkos realijas, kadangi vertinimo sistemos neatitikimas realybei ir jos nesugebėjimas įnešti pokyčių gali trukdyti organizacijos tolimesnei raidai ir progresui.

Apibendrinant galima teigti, kad veiklos efektyvumo vertinimas organizacijos veikloje yra tiek pat svarbus, kaip ir kitos kibernetinio saugumo valdymo modelio dalys, nes jis įgalina organizaciją keistis ir tobulėti, siekiant savo užsibrėžtų tikslų, o jo nebuvimas kelia pavojų bet kokiai organizacijos veiklai bei daro organizacijos pastangas, diegiant kibernetinio saugumo valdymo modelį, bevaises.

3.2.9. Kibernetinio saugumo valdymo modelio apibendrinimas

Atlikus sukurto bei pagal kibernetinio saugumo ekspertų empirinio tyrimo metu pateiktus atsakymus ir pastebėjimus patikslinto kibernetinio saugumo valdymo modelio struktūros analizę ir apibendrinant šioje disertacinio darbo dalyje aptariamas modelio dimensijų įgyvendinimo priemones ir lygius, būtina pažymėti, kad sukurto kibernetinio saugumo valdymo modelio taikymas yra tinkamas ne tik elektroninių balsavimo sistemų konstravimo, diegimo, valdymo ir naudojimo procesuose, kurie gali palengvinti saugių elektroninių rinkimų sistemų atsiradimą ir panaudojimą demokratiniams procesams užtikrinti, bet ir siekiant įgyvendinti kibernetinio saugumo valdymą ir kitose organizacijose.

Tikėtina, kad, naudojant disertacijos autoriaus sukurtą kibernetinio saugumo valdymo modelį elektroninių rinkimų sistemų kibernetiniam saugumui užtikrinti, šios sistemos taps labiau suprantamos ne tik tam tikroms suinteresuotoms organizacijoms, bet ir paprastiems piliečiams, padidins valstybių piliečių politinį aktyvumą bei jų pasitikėjimą valstybės teikiamomis elektroninio balsavimo paslaugomis ir galimybėmis.

Tačiau būtina pažymėti, kad šiame disertaciniame darbe sukurtas ir aptartas kibernetinio saugumo valdymo modelis atspindi tik bendrą globalų valstybės arba jai atstovaujančių organizacijų požiūrį į kibernetinį saugumą ir jo valdymą, nesigilinant į konkrečias kibernetinio saugumo valdymo technikas bei saugumo kompanijų siūlomus technologinius sprendimus. Nagrinėjant konkrečias technologines, administracines ir teisines priemones, kuriomis turi būti užtikrinamas kibernetinis saugumas organizacijos valdomose informaciniuose ištekliuose, būtina naudoti ne tik šį kibernetinio saugumo valdymo modelį, kuris iš esmės yra tam tikras kibernetinio saugumo valdymo organizacinis „karkasas“, bet ir būtinai pasinaudoti gerosiomis kibernetinio saugumo valdymo praktikomis (standartais, technikomis ir kt.), kurių paskirtis yra siejama su konkrečių technologinių, rizikos ir incidentų valdymo ar kitų kibernetinio saugumo klausimų sprendimo būdais.

Kaip jau buvo paminėta anksčiau, šio disertacinio darbo metu sukurtas kibernetinio saugumo valdymo modelis yra skirtas visapusiškam organizacijos kibernetiniam saugumui valdyti ir užtikrinti, atsižvelgiant į visus organizacijos vykdomus veiklos procesus ir valdomus išteklius. Vien tik technologinis kibernetinis saugumas, kuriam užtikrinti panaudojamos techninės ir programinės priemonės, negarantuoja kibernetinio saugumo organizacijos valdomose informaciniuose ištekliuose, kadangi bet kokia technologija anksčiau ar vėliau gali būti pažeidžiama. Tik konceptualus požiūris į kibernetinį saugumą ir jo valdymą, įtraukiant į valdymo procesą ne tik technologinius aspektus, bet ir organizacijos personalą, aukščiausio lygio vadovus, paslaugų tiekėjus ir partnerius, organizaciją supančias aplinkas, galimas rizikas ir incidentus, garantuoja kibernetinio saugumo lygio padidėjimą organizacijoje, taip pat prisideda prie globalaus kibernetinio saugumo lygio užtikrinimo valstybėje.

Pažymėtina, kad *iš visų šešių kibernetinio saugumo valdymo modelyje nagrinėjamų dimensijų* (*organizacijos valdymas, teisinis reguliavimas, kibernetinio saugumo kultūra, technologinis saugumas, rizikų ir incidentų valdymas) neįmanoma išskirti vienos pačios svarbiausios, kadangi tik visų* šešių kibernetinio saugumo *valdymo dimensijų priemonių įdiegimas organizacijoje bei šių dimensijų sujungimas į vieną bendrą organizacijos kibernetinio saugumo valdymo sistemą gali parodyti aiškius kibernetinio saugumo pokyčio rezultatus*. Kaip ir buvo minėta anksčiau, kiekviena modelio dimensija gali būti vystoma atskirai, numatant skirtingus pirmojo ir antrojo lygio priemonių įgyvendinimo laikus, atsižvelgiant į organizacijos veiklos ypatumus, valdomus išteklius, turimus resursus bei finansines galimybes. Tačiau būtina pažymėti, kad visų kibernetinio saugumo valdymo modelio dimensijų trečiasis lygmuo yra siejamas su pavienių ir tarpusavyje nepriklausomų organizacijos kibernetinio saugumo valdymo procesų (dimensijų) virsmu į integruotą kibernetinio saugumo valdymo sistemą, kurios komponentai yra vienareikšmiškai susieti bei veikia vienas kitą (žr. 20 paveikslą).

Būtina paminėti, kad sėkmingam kibernetinio saugumo valdymo modelio taikymui organizacija turi sukurti ir naudoti kibernetinio saugumo gerinimo veiklos efektyvumo vertinimo sistemą. Šioje sistemoje turi būti aiškiai numatyti kiekvienos kibernetinio saugumo valdymo modelio dimensijos vertinimo kriterijai bei būdai, kuriais bus matuojamas organizacijos kibernetinio saugumo efektyvumo pokytis, o pati sistema, kaip ir buvo minėta anksčiau, padės vienareikšmiškai nustatyti kibernetinio saugumo situacijos kaitą organizacijoje bei nurodys silpniausias kibernetinio saugumo valdymo proceso grandis.

Apibendrinant šį disertacinio darbo skyrių, galima teigti, kad kibernetinio saugumo valdymo modelis, aprašytas šioje disertacinio darbo dalyje, visose modelio dimensijose nagrinėja teisines, informacijos sklaidos, organizacines ir technines kibernetinio saugumo valdymo ir užtikrinimo priemones, kurių paskirtis yra išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos saugumui, kaip yra minima Lietuvos Respublikos 2018 metų Kibernetinio saugumo įstatyme. Pažymėtina, kad šis kibernetinio saugumo valdymo modelis gali būti naudojamas ne tik elektroninio balsavimo sistemų kibernetinio saugumo valdymo ir užtikrinimo kontekste, bet ir bet kokios kitos organizacijos, siekiančios pagerinti savo kibernetinį saugumą ir jo valdymą bei įgyti atsparumą šiuolaikinėms kibernetinėms grėsmėms.

IŠVADOS IR REKOMENDACIJOS

1. Atlikus mokslinių šaltinių analizę, siekiant atskleisti kibernetinio saugumo valdymo teorinius aspektus bei įvardyti pagrindines kibernetinio saugumo incidentų atsiradimo priežastis ir ypatumus, kibernetinio saugumo valdymo problematiką bei galimą kibernetinio saugumo incidentų įtaką ir poveikį elektroninių rinkimų sistemų kibernetiniam saugumui, nustatyta kad:
   1.1. Kibernetinio saugumo apibrėžimų įvairovė suponuoja šio reiškinio suvokimo problematiką ne tik visuomenės sluoksniuose, kasdien tiesiogiai nesusiduriančiose su šiuo reiškiniu, bet ir tarp asmenų, kurie tiesiogiai dirba su kibernetinio saugumo užtikrinimo iššūkiais. Šiuolaikinis kibernetinis saugumas turi būti traktuojamas ne tik kaip technologinė disciplina, bet kaip vientisas sudėtingas reiškinys, kuriame yra nagrinėjami techniniai, teisiniai, personalo, organizacijos valdymo ir kitų mokslų aspektai;
   1.2. Informacinių ir ryšio technologijų skvarbos ir jų įtakos įvairioms visuomenės gyvenimo sritims didėjimas sudaro sąlygas kibernetinio saugumo grėsmių augimui ir sėkmingų kibernetinių atakų skaičiaus padidėjimui;
   1.3. Organizacijų pasitikėjimas esama valdomos infrastruktūros apsauga, informacinių sistemų aptarnaujančio personalo žiniomis, naudojama technologine įranga ir jos atliekamomis funkcijomis bei supančios aplinkos suvokimo problematika sukelia galimybes rengti sėkmingas kibernetines atakas prieš organizacijas ir sistemas;
   1.4. Šiuolaikiniame technologijomis grindžiamame pasaulyje keičiasi ne tik kibernetinio saugumo incidentų ir grėsmių rūšys, bet tobulėja ir kibernetinių incidentų sukėlėjų naudojamos atakų vykdymo priemonės. Atsiranda naujos atakų rūšys, kurių tikslas yra tiesiogiai nesusijęs su technologinių priemonių panaudojimu, siekiant diskredituoti informacines sistemas ar jų teikiamas paslaugas;
   1.5. Nors technologiniai kibernetinio saugumo pažeidžiamumai šiuolaikiniame pasaulyje ir yra laikomi viena iš svarbiausių saugumo pažeidžiamumų rūšimi, dabartiniu laikotarpiu vis dažniau žmogiškasis faktorius yra įvardijamas kaip priežastis, dėl kurios dažniausiai yra sėkmingai įgyvendinamos kibernetinės atakos. Siekiant apsaugoti informacinius išteklius nuo žmogiškojo faktoriaus įtakos, yra būtinas ne tik technologinių priemonių panaudojimas, bei šių priemonių automatizavimas, bet ir veiksmai, kuriais bus minimizuojama žmogiškojo faktoriaus įtaka kibernetiniam saugumui;
   1.6. Disertacinio darbo pirmojoje teorinėje dalyje nagrinėti pasaulyje naudojami organizacijų kibernetinio saugumo valdymo modeliai labiausiai yra orientuoti į technologinio kibernetinio saugumo užtikrinimą organizacijoje, tačiau modeliuose visiškai neaptariami arba menkai aptariami organizacijos, žmogiškųjų išteklių, rizikos ir incidentų valdymo aspektai;
   1.7. Atlikus kibernetinio saugumo incidentų, atakų ir galimų pažeidžiamumų analizę elektroninių rinkimų sistemų kontekste, disertacijoje yra pristatoma

elektroninių rinkimų sistemų kibernetinių incidentų taksonomija, kurioje yra išsamiai nagrinėjami ne tik tradiciniai kibernetinių atakų būdai, bei jos vykdantys asmenys, bet ir klasifikuojami kibernetinių nusikaltėlių tikslai, atakų taikiniai bei jų vykdymo būdai;

1.8. Valdymo sistemos sukūrimas ir pritaikymas elektroninių balsavimo sistemų konstravimo procese gali sudaryti galimybes eliminuoti daugumą nustatytų ir disertaciniame darbe aptartų pažeidžiamumų.

2. Teorinių įžvalgų pagrindu kuriant konceptualų kibernetinio saugumo valdymo modelį, kuris gali būti taikomas elektroninių rinkimų sistemų konstravimo, diegimo, valdymo ir naudojimo procesų metu, nustatyta, kad:
   2.1. Siekiant tinkamo kibernetinio saugumo valdymo organizacijoje, būtina nagrinėti šešias saugumo dimensijas: organizacijos valdymo procesų, teisinio reguliavimo, kibernetinio saugumo kultūros, technologinio saugumo, rizikos ir incidentų valdymo;
   2.2. Kibernetinio saugumo grėsmių valdymas, pasinaudojant šių dimensijų įgyvendinimo priemonėmis, gali padėti organizacijai sėkmingai kontroliuoti galimas rizikas ir pažeidžiamumus bei sumažinti sėkmingų kibernetinių išpuolių poveikį valdomiems ištekliams;
   2.3. Didžiausias iššūkis yra susijęs su technologinių žinių ir valdymo procesų sujungimu, nes dažniausiai techninis personalas ir valdymo specialistai skirtingai traktuoja kibernetinio saugumo valdymo aspektus;
   2.4. Organizacijos pokyčiai kibernetinio saugumo kontekste prasideda tuomet, kai saugumas organizacijoje pradedamas traktuoti ne tik kaip technologinė disciplina, bet kaip realus valdymo sistemos kaitos iššūkis;
   2.5. Kibernetinio saugumo valdymo modelis taip pat suteikia galimybę organizacijos lyderiams aktyviai dalyvauti, priimant sprendimus ir kuriant kibernetinio saugumo politiką, bei įgalina organizaciją tinkamai vertinti saugumo rizikas ir jų mažinimo priemones;
   2.6. Kibernetinio saugumo valdymo modelio įdiegimas taip pat gerina organizacijos reputaciją išorinėje aplinkoje, nes organizacija, kuri rūpinasi savo kibernetiniu saugumu, yra patrauklesnė vartotojams ar verslo partneriams;
   2.7. Disertaciniame darbe siūlomo valdymo modelio idėja ir aktualumas yra siejami su naujo požiūrio į kibernetinį saugumą formavimu, kuomet jis yra taikomas visos organizacijos veiklos procesams, o kiekvienas organizacijos narys privalo dalyvauti kibernetinio saugumo gerinime;
   2.8. Organizacijos izoliavimas nuo išorinio pasaulio ir jame egzistuojančių kibernetinių grėsmių yra neįmanomas, o diegiamas kibernetinio saugumo valdymo modelis turi nagrinėti ne tik organizacijos vidaus aplinką, bet ir jos sąveiką su išorine aplinka.

3. Atlikus empirinio tyrimo metu siūlomo kibernetinio saugumo valdymo modelio vertinimą bei apibendrinus pusiau struktūrizuoto ekspertų interviu metu gautus rezultatus, nustatyta, kad:

3.1. Siūlomo kibernetinio saugumo valdymo modelio komponentai: organizacijos valdymo procesų, teisinio reguliavimo, kibernetinio saugumo kultūros, technologinio saugumo, rizikos ir incidentų valdymo dimensijos, turi būti naudojami kuriant kibernetinio saugumo valdymą;
3.2. Siūlomas modelis turintis veiklos efektyvumo vertinimo sistemą, suteikia organizacijai galimybę stebėti kibernetinio saugumo valdymo įgyvendinimo pokyčius konkrečiose dimensijose, taip pat nustatyti organizacijos kibernetinio saugumo valdymo evoliucionavimo procesą;
3.3. Siūlomo kibernetinio saugumo valdymo modelio įgyvendinimas tūri būti atliekamas laipsniškai (pakopomis, lygiais);
3.4. Organizacijos valdymo procesų dimensijos įtaka saugumo kūrimui organizacijoje gali būti apibūdinama kaip lemiamas kibernetinio saugumo valdymo įgyvendinimo procesas. Organizacijos vykdomos veiklos koregavimas ir pritaikymas kibernetinio saugumo procesams užtikrinti keičia organizacijos veiklos modelį bei atveria galimybes pažeidžiamumams mažinti;
3.5. Teisinis reguliavimas yra neatsiejamas nuo kibernetinio saugumo valdymo. Šios dimensijos ribose yra užtikrinamas organizacijos teisinio reglamentavimo sukūrimas, suteikiantis organizacijai galimybę administracinėmis priemonėmis didinti vidinės organizacijos aplinkos atsparumą kibernetinėms grėsmėms;
3.6. Įgyvendindama teisinio reguliavimo dimensiją, organizacija taip pat turi galimybę daryti įtaką ne tik vidinei, bet ir išorinei aplinkai, dalyvaujant kibernetinio saugumo teisinės bazės rengimo procese;
3.7. Siekiant sumažinti organizacijos pažeidžiamumą bei išvengti kibernetinių incidentų, yra privalomas visų, be išimties, darbuotojų mokymas ir švietimas, nepaisant darbuotojo užimamų pareigų. Toks kompleksinis požiūris suteikia galimybes eliminuoti galimas grėsmes (atakas), neatsižvelgiant į tai, į kokią personalo grupę jos yra orientuotos;
3.8. Bendradarbiaujant su partneriais, paslaugų tiekėjais, kitomis organizacijomis, būtina vertinti galimų partnerių kibernetinio saugumo valdymą, tokiu būdu sudarant galimybę išvengti savo valdomos infrastruktūros kompromitavimo bei galimų nuostolių;
3.9. Technologinis kibernetinis saugumas turi būti siejamas ne su konkrečių technologinių sprendimų parinkimu organizacijos saugumui užtikrinti, o vykdomas kaip technologiškai neutralus įrangos ir kibernetinio saugumo sprendimų valdymo procesas, numatantis būtinus organizacijos veiksmus, siekiant užtikrinti vykdomos veiklos tęstinumą, įrangos gyvavimo ciklo palaikymą, išteklių planavimą ir kt.;
3.10. Tik tinkamas rizikos įvertinimas, klasifikavimas bei jų mažinimo priemonių identifikavimas suteikia organizacijai galimybę nusimatyti galimų pažeidžiamumų vengimo ar mažinimo strategiją, subalansuojant ir minimizuojant šiam procesui skiriamus finansinius išteklius;

3.11. Kibernetinių incidentų valdymas organizacijoje turi būti suprantamas ne kaip reagavimas į vykstančią kibernetinę ataką ar jos padarinių šalinimas, bet kaip nenutrūkstamas procesas, kurio metu yra vertinama ne tik vidinė organizacijos valdoma infrastruktūra, bet ir išorės aplinka: kibernetinių incidentų plėtros tendencijos, atakų atlikimo metodai ir būdai, technologinių atakų alternatyvos ir kt.;

3.12. Tinkamas kibernetinio saugumo kultūros kūrimas ne tik organizacijoje, bet visos valstybės mastu, gali tapti visuotinio kibernetinio saugumo pagerėjimo priežastimi, bet šie gebėjimai privalo būti ugdomi visuose lygmenyse, pradedant nuo švietimo sistemos pradinio ugdymo programų;

3.13. Sukurti saugią elektroninių rinkimų sistemą yra įmanoma, tik įtikinus šios sistemos naudotojus (piliečius), kad jų balsai, atiduoti technologijomis grindžiama rinkimų sistema, nebus suklastoti, o rinkimų rezultatais nebus manipuliuojama;

3.14. Būtina tinkamai informuoti visuomenę, siekiant tinkamo visuomenės nuomonės apie elektroninius rinkimus susiformavimo. Nuomonės formavimas viešoje erdvėje, į kurį yra įtrauktos pilietinės visuomenės organizacijos, valstybės ir savivaldybių atstovai, medija, kibernetinio saugumo ekspertai ir kitos suinteresuotosios asmenų grupės, gali paskatinti visuomenę maksimaliai pasitikėti elektroniniais balsavimais, ir paspartinti šios sistemos įdiegimą, kas yra ypač aktualu dabartiniais pandemijos laikais.

LITERATŪRA

Teisės aktai

1. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas), <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679 >.
2. Lietuvos Respublikos Kibernetinio saugumo įstatymas Nr. XII-1428 (2014), <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/WlhuElQgvR>.
3. Lietuvos Respublikos Kibernetinio saugumo įstatymo pakeitimo įstatymas (2018), <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/15e540727ac211e89188e16a6495e98c>.
4. Lietuvos Respublikos Konstitucija, <https://www.e-tar.lt/portal/lt/legalAct/TAR.47BB952431DA/UwoGawiEom>.
5. Lietuvos Respublikos seimo nutarimas Nr. XI-2131 Dėl Lietuvos Respublikos seimo nutarimo „Dėl nacionalinio saugumo strategijos patvirtinimo“ pakeitimo, < https://www.e-tar.lt/portal/lt/legalAct/TAR.FD615B2F7F90>.
6. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas, <https://e-seimas.lrs.lt/portal/legalActEditions/lt/TAD/TAIS.91654?faces-redirect=true>.

Mokslinės literatūros šaltiniai:

7. Ackermann T., 2012. Perceived IT Security Risks in the Context of Cloud Computing, IT Security Risk Management, Springer, ISBN: 978-3-658-01114-7, <https://doi.org/10.1007/978-3-658-01115-4>.
8. Agrawal M.; Campoe A.; Pierce E., 2014. Information Security and IT Risk Management, John Wiley & Sons, ISBN 978-1-118-33589-5.
9. Alotaibi M.; Furnell S.; Clarke N., 2016. Information security policies: A review of challenges and influencing factors, 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, 2016, <https://doi.org/10.1109/ICITST.2016.7856729>.
10. Alvarez R. M.; Hall T. E., 2010. Electronic Elections: The Perils and Promises of Digital Democracy, ISBN: 9780691146225.
11. Anderson R., 2001. Why information security is hard – an economic perspective, 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, <https://www.acsac.org/2001/papers/110.pdf>.
12. Appazov A., 2014. Legal Aspects of Cybersecurity, University of Copenhagen, <http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf >.
13. Aranha D. F.; Karam M. M.; de Miranda A.; Scarel F., 2014. Software vulnerabilities in the Brazilian voting machine. In Design, Development, and Use of Secure Electronic Voting Systems, <http://dx.doi.org/10.4018/978-1-4666-5820-2.ch008>.

14. Ashenden D, 2008. Information Security management: A human challenge?, <http://dx.doi.org/10.1016/j.istr.2008.10.006>.
15. Augoye V.; Tomlinson A., 2018. Analysis of electronic voting schemes in the real world, <https://www.ukais.org/resources/Documents/ukais2018proceedingspapers/paper_17.pdf>.
16. Augustinaitis A.; Rudzkienė V.; Petrauskas R. A.; Dagytė I.; Martynaitytė E.; Leichteris E.; Malinauskienė E.; Višnevska V.; Žilionienė I., 2009. Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas, kolektyvinė monografija, Mykolo Romerio universitetas, ISBN 9789955191605.
17. Bakshi T.; Papadaki M.; Furnell S., 2009. Social engineering: assessing vulnerabilities in practice. Information Management & Computer Security, vol. 17 (1), p. 53–63, <https://doi.org/10.1108/09685220910944768>.
18. Baležentis A.; Žalimaitė M., 2011. Ekspertinių vertinimų taikymas inovacijų plėtros veiksnių analizėje: Lietuvos inovatyvių įmonių vertinimas, Management theory and studies for rural business and infrastructure development, 2011 Nr. 3(27). ISSN 1822-6760, <http://mts.asu.lt/mtsrbid/article/viewFile/269/298>.
19. Barnes K., Johnson B., Nickelson R.; 2004. Introduction to SCADA protection and vulnerabilities, <http://dx.doi.org/10.2172/911209>.
20. Bedeian A. G.; Wren D. A., 2009. The Evolution of Management Thought.
21. Beissel S., 2016. Cybersecurity Investments: Decision Support Under Economic Aspects, Springer, ISBN 978-3-319-30460-1.
22. Bernier M., 2013. Military Activities and Cyber Effects (MACE) Taxonomy, Defence R&D Canada, Centre for Operational Research and Analysis.
23. Bitici U. S.; Carrie A. S.; McDevitt L., 1997. Integrated performance measurement systems: a development guide. International Journal of Operations & Production Management, 1997, p. 522-534, ISSN 0144-3577.
24. Blasch E.; Al-Nashif Y.; Hariri S., 2014. Static versus Dynamic Data Information Fusion analysis using DDDAS for Cyber Security Trust, Procedia Computer Science, (29) 2014, <http://fs.unm.edu/StaticVersusDynamicData.pdf>.
25. Bologna S.; Fasani A.; Martellini M., 2013. Cyber Security and Resilience of Industrial Control Systems and Critical Infrastructures, Cyber Security Deterrence and IT Protection for Critical Infrastructures, Springer, ISBN 978-3-319-02278-9.
26. Bossong R.; Wagner B., 2018. A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union. In: Bures O., Carrapico H. (eds) Security Privatization. Springer, Cham. <https://doi.org/10.1007/978-3-319-63010-6_10>.
27. Brar H. S.; Kumar G., 2018. Cybercrimes: A Proposed Taxonomy and Challenges. Journal of Computer Networks and Communications, Volume 2018, <https://doi.org/10.1155/2018/1798659>.
28. Brenner S. W., 2013. Cyber-Threats and the Limits of Bureaucratic Control, Minnesota Journal of Law, Science, and Technology, 14 (2013), <http://purl.umn.edu/144222>.
29. Brightwell I.; Cucurull J.; Galindo D.; Guasch S., 2015. An overview of the iVote 2015 voting system, <https://www.elections.nsw.gov.au/__data/assets/pdf_file/0019/204058/An_overview_of_the_iVote_2015_voting_system_v4.pdf>.

30. Brisch K., 2017. The Law and Its Contribution to IT Security: Legal Framework, Requirements, Limits. Cyber Security. Simply. Make it Happen, Springer, ISBN 978331946528-9.
31. Bryman A., 2001. Social research methods, 4th edition, Oxford University Press Inc., 2012, ISBN 9780199588053.
32. Burns T.; Stalker G. M., 1961. The Management of Innovation, Oxford University Press Inc., 1994, ISBN 9780198288787.
33. Cancian F. M., 1972. The System Of Modern Societies. By Talcott Parsons, Social Forces, Vol. 51 (1), <https://doi.org/10.1093/sf/51.1.104>.
34. Caravelli J.; Jones N., 2019. Cyber Security: Threats and Responses for Government and Business, ISBN 9781440861734.
35. Cayirci E.; Ghergherehchi R., 2011. Modeling cyber attacks and their effects on decision process, Proceedings of the 2011 Winter Simulation Conference, <https://doi.org/10.1109/WSC.2011.6147970>.
36. Chang C. K., 2016. Situation Analytics: A Foundation for a New Software Engineering Paradigm, Iowa State University, <http://www.sigdrm.org/~zzhang/data/Situation-Analytics-A-Foundation-for-a-New-Software-Engineering-Paradigm.pdf>.
37. Chen J.; Pedrycz W.; Ma L.; Wang C., 2014. A new information security risk analysis method based on membership degree. Kybernetes 43(5), <https://doi.org/10.1108/K-10-2013-0235>.
38. Chowdhury M. J. M., 2013. Comparison of e-voting schemes: Estonian and Norwegian solutions, International Journal of Applied Information Systems 6(2), <https://courses.cs.ut.ee/2010/security-seminar-fall/uploads/Main/chowdhury-final.pdf>.
39. Cohen F., 2015. Protection and Engineering Design Issues in Critical Infrastructures, Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, CRC Press, ISBN-13: 978-1-4822-3923-2.
40. Coram P.; Ferguson C.; Moroney R., 2006. The value of internal audit in fraud detection. J. Account. Financ. 48(4), <https://www.researchgate.net/profile/Colin_Ferguson4/publication/253527357_The_Importance_of_Internal_Audit_in_Fraud_Detection/links/00b7d52990006b43e4000000/The-Importance-of-Internal-Audit-in-Fraud-Detection.pdf>.
41. Craig A.; Valeriano B., 2016. Reacting to Cyber Threats: Protection and Security in the Digital Age, Global Security and Intelligence Studies: Vol. 1: No. 2, Article 4, <http://digitalcommons.apus.edu/gsis/vol1/iss2/4>.
42. Cucu P., 2017. How every cyber attack works – A full list. Heimdal Security. <https://heimdalsecurity.com/blog/cyber-attack/#>.
43. Dalziel H., 2016. Cyber Security Awareness for CEOs and Management, ISBN: 978-0-12-804754-5, Elsevier Inc.
44. Dykstra J., 2017. Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems.
45. Evans M.; Maglaras L.; He Y.; Janicke H., 2016. Human Behaviour as an aspect of Cyber Security Assurance, Security and Communication Networks 9(17), <https://doi.org/10.1002/sec.1657>.

46. Fayol H., 1916. General and industrial management, translation from French, Sir Isaac Pitman & Sons Ltd., London.
47. Fayol H. Administravimas: teorija ir praktika. Vilnius. Eugrimas, 2005.
48. Ferdinand J.; Benham R., 2017. The cyber security ecosystem: defining a taxonomy of existing, emerging and future cyber threats, SWIFT Institute.
49. Fernando S., 2018. The Different Aspects of Information Security Education, Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution, ISBN 9781522547631.
50. Furnell S.; Fischer P.; Finch A., 2017. Can't get the staff? The growing need for cyber-security skills, Computer Fraud and Security (2) (2017), pp. 5-10.
51. Freiling F. C.; Schwittay B., 2007. A Common Process Model for Incident Response and Digital Forensics, Conference on IT Incident Management and IT Forensics (IMF2007), Stuttgart.
52. Fieldman A. J.; Halderman J. A.; Felten E. W., 2006. Security Analysis of the Diebold AccuVote-TS Voting Machine, <http://citp.princeton.edu/pub/ts06full.pdf>.
53. Franco-Santosa M.; Lucianettib L.; Bournea M., 2012. Contemporary performance measurement systems: A review of their consequences and a framework for research, Management Accounting Research, <https://doi.org/10.1016/j.mar.2012.04.001>.
54. Frangopoulos E. D.; Eloff M.M.; Venter L. M., 2008. Social aspects of information security, Conference: Proceedings of the ISSA 2008 Innovative Minds Conference, ISSA 2008, Gauteng Region (Johannesburg), South Africa, 7-9 July 2008.
55. Galinec D.; Možnik D.; Guberina B., 2017. Cybersecurity and cyber defence: national level strategic approach, Automatika, 58:3, <https://doi.org/10.1080/00051144.2017.1407022>.
56. Geers K., 2015. Coder, Hacker, Soldier, Spy, Cyber Security: Analytics, Technology and Automation, ISBN 978-3-319-18301-5.
57. Gerth H. H.; Mills C. W., 1958. From Max Weber: Essays in Sociology.
58. Gleghorn G.; Gordon J., 2012. A quantitative examination of perceived promotability of information security professionals with vendor-specific certifications versus vendor-neutral certifications, Research in Business and Economics Journal, 6 (2012).
59. Goldsmith B., 2017. Guidelines for Trialling E-Voting in National Elections. Real-World Electronic Voting: Design, Analysis and Deployment, CRC press, ISBN: 978-1-4987-14693.
60. Gomes C. F.; Yasin M. M., 2011. A systematic benchmarking perspective on performance management of global small to medium-sized organizations: An implementation-based approach», Benchmarking: An International Journal, <https://core.ac.uk/download/pdf/19133793.pdf>.
61. Gonggrijp R.; Hengeveld W-J., 2007. Studying the Nedap/Groenendaal ES3B voting computer: a computer security perspective, <https://www.usenix.org/legacy/events/evt07/tech/full_papers/gonggrijp/gonggrijp.pdf>.
62. Govindarasu M., Hahn A., 2017. Cybersecurity of the Power Grid: A Growing Challenge, <https://www.usnews.com/news/national-news/articles/2017-02-24/cybersecurity-of-the-power-grid-a-growing-challenge>.

63. Granneman S., 2003. Linux vs. Windows Viruses: Let›s go to work, <https://www.theregister.co.uk/2003/10/06/linux_vs_windows_viruses>.
64. Gruschka N,; Jensen M., 2010. Attack Surfaces: A Taxonomy for Attacks on Cloud Services. 2010 IEEE 3rd International Conference on Cloud Computing.
65. Gupta B. B.; Perez G. M.; Agrawal D. P.; Gupta D., 2020. Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Springer, ISBN 978-3-030-22276-5.
66. Hadlington L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours, Heliyon, 3(7)2017, <https://doi.org/10.1016/j.heliyon.2017.e00346>.
67. Haqaf, H.; Koyuncu M., 2018. Understanding key skills for information security managers. International Journal of Information Management, 43 (2018).
68. Halderman J. A., 2017. Practical Attacks on Real-World E-Voting. Real-World Electronic Voting: Design, Analysis and Deployment, CRC press, ISBN: 9781498714693.
69. Halderman J. A.; Teague V., 2015. The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election, Washington, D.C., USENIX Association.
70. Hampden-Turner C.; Trompenaars F., 2011. Riding the Waves of Culture - Understanding Diversity in Global Business, ISBN 1904838405.
71. Hansman S.; Hunt R., 2003. A taxonomy of network and computer attack methodologies.
72. Harrison K.; White G., 2011. A Taxonomy of Cyber Events Affecting Communities, Proceedings of the 44th Hawaii International Conference on System Sciences.
73. Harry C., 2018. A Proposed Hierarchical Taxonomy for Assessing the Primary Effects of Cyber Events: A Sector Analysis 2014-2016, University of Maryland.
74. Houston N., 2019. The Impact of Human Behavior on Cyber Security: Concepts, Methodologies, Tools, and Applications, Multigenerational Online Behavior and Media Use, <https://doi.org/10.4018/978-1-5225-7909-0.ch068>.
75. Howard J.D.; Longstaff T. A., 1998. A Common Language for Computer Security Incidents, Sandia Report.
76. Hui P.; Bruce J.; Fink G.; Gregory M.; Best B.; McGrath L.; Endert A., 2010 «Towards efficient collaboration in cyber security,» 2010 International Symposium on Collaborative Technologies and Systems, Chicago, 2010, <https://doi.org/10.1109/CTS.2010.5478473>.
77. Hursti H., 2006. Critical security issues with Diebold TSx, <https://www.blackboxvoting.org/BBVtsxstudy.pdf>.
78. Jastiuginas S., 2011. Informacijos saugumo valdymas Lietuvos viešajame sektoriuje. Informacijos mokslai, 2011 (5), <http://www.zurnalai.vu.lt/informacijos-mokslai/article/view/3137/2261>.
79. Jefferson D.; Rubin A. D.; Simons B.; Wagner D., 2004. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE).

80. Jenab K., Moslehpour S., 2016. Cyber Security Management: A Review. Business Management Dynamics, Vol.5, No.11, p. 16-39.
81. Johnson T. A., 2015. Cybersecurity Threat Landscape and Future Trends. Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, CRC Press, ISBN-13: 978-1-4822-3923-2.
82. Johnson T. A., 2015. Economic Cost of Cybersecurity, Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, CRC Press, ISBN-13: 978-1-4822-3923-2.
83. Johnson T. A., 2015. Historical Reference Points in the Computer Industry and Emerging Challenges in Cybersecurity, Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, CRC Press, ISBN-13: 978-1-4822-3923-2.
84. Jones K. K., 2013. The Impact of Legislation on the Organization: Evaluating the Impact of Corporate Governance Regulation on the Internal Audit Function.Dissertation, Georgia State University, <https://scholarworks.gsu.edu/bus_admin_diss/22>.
85. Kacha P., 2016. IDEA: Security Event Taxonomy Mapping, Advances in Information Science and Applications, Proceedings of the 18th International Conference on Computers, Santorini Island, Greece.
86. Kaplan J. M., 2017. Cybersecurity for commercial advantage, Handbook of System Safety and Security, Elsevier, ISBN 978-0-12-803773-7.
87. Kaplan R. S.; Norton D. P., 2001. The strategy-focused organization: how balanced scorecard companies thrive in the new business environment, Stewart&Co., ISBN 157851250-6.
88. Karda S.; Kiraz M. S.; Bingöl M. A.; Birinci F., 2016. Norwegian internet voting protocol revisited: ballot box and receipt generator are allowed to collude, <https://onlinelibrary.wiley.com/doi/pdf/10.1002/sec.1678>.
89. Kardelis K., 2017. Mokslinių tyrimų metodologija ir metodai, Mokslo ir enciklopedijų leidybos centras, ISBN 978-5-420-01771-5.
90. Kaspar L.; Shears M., 2017. A Multistakeholder Approach To Cybersecurity Policy Development, European cybersecurity journal 3(2017), <https://www.gp-digital.org/wp-content/uploads/2017/10/ECJ-Volume3.Issue3-Extract-KASPAR-and-SHEARS.pdf>.
91. Kiayias A.; Michel L.; Russell A.; Shvartsman A. A., 2006. Security Assessment of the Diebold Optical Scan Voting Terminal, UConn Voting Technology Research Center. < https://voter.engr.uconn.edu/voter/wp-content/uploads/uconn_report-os.pdf>.
92. Kjaerland M., 2006. A taxonomy and comparison of computer security incidents from the commercial and government sectors. Computers and Security, Vol. 25.
93. Kefalas A.G., 1981. Analyzing changes in the external business environment, Planning Review, Vol. 9 (4), <https://doi.org/10.1108/eb053956>.
94. Kessler E. H., 2013. Encyclopedia of management theory, SAGE Publications, Inc.
95. Kennerley M.; Neely A., 2002. A framework of the factors affecting the evolution of performance measurement systems, International Journal of Operations

& Production Management, <https://www.emeraldinsight.com/doi/full/10.1108/01443570210450293>.
96. Kiškis M., Limba T., 2016. Biotechnology Patenting in Small Countries—Strategies for the International Marketplace. Biotechnology Law Report 35(6): p. 291-299, <http://doi.org/10.1089/blr.2016.29035.mk>.
97. Kiškis M., Limba T., Gulevičiūtė G., 2016. Business Value of Intellectual Property in Biotech SMEs: Case Studies of Lithuanian and Arizona's (US) Firms. Entrepreneurship and Sustainability Issues 4(2): p. 221-234, <http://dx.doi.org/10.9770/jesi.2016.4.2(11)>.
98. Knapp K. J.; Marshall T. E.; , Rainer R. K.; Morrow D. W., 2006. The Top Information Security Issues Facing Organizations: What Can Government Do to Help?, The EDP Audit, Control, and Security Newsletter (EDPACS), 34:4, 1-10, <https://doi.org/10.1201/1079.07366981/46351.34.4.20061001/95104.1>.
99. Kohno T.; Stubblefield A.; Rubin A. D.; Wallach D. S., 2004. Analysis of an electronic voting system. In IEEE Symposium on Security and Privacy, <http://avirubin.com/vote.pdf>.
100. Kosseff J., 2018. Developing Collaborative and Cohesive Cybersecurity Legal Principles, 2018 10th International Conference on Cyber Conflict CyCon X: Maximising Effects, NATO CCDCOE, <https://ccdcoe.org/uploads/2018/10/Art-15-Developing-Collaborative-and-Cohesive-Cybersecurity-Legal-Principles.pdf>.
101. Kosseff J., 2020. U.S. Government Cyber Structure and Public–Private Cybersecurity Partnerships, Cybersecurity Law, 2nd ed., ISBN 9781119517290, Wiley.
102. Kovacich G., 2016. The Information Systems Security Officer's Guide: Establishing and Managing a Cyber Security Program, Elsevier, ISBN: 9780128021903.
103. Kroger W., 2008. Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools, Reliability Engineering and System Safety, 93 (2008), 1781–1787, <http://dx.doi.org/10.1016/j.ress.2008.03.005>.
104. Lackram J.; Padayachee I., 2018. Social Engineering in Information Security Breaches and the Factors That Explain Its Success: An Organizational Perspective, Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution, ISBN 9781522547631.
105. Lahcen R. A.; Caulkins B.; Mohapatra R.; Kumar M., 2020. Review and insight on the behavioral aspects of cybersecurity, Cybersecur 3, 10 (2020), <https://doi.org/10.1186/s42400-020-00050-w>.
106. Landwehr C. E.; Bull A.; McDermott J.; Choi W., 1994. A taxonomy of computer program security flaws, with examples. ACM Computing Surveys.
107. Libby R.; Blashfield R. K., 1978. Performance of a composite as a function of the number of judges. Organizational Behavior & Human Performance, 21(2), 121-129, <https://doi.org/10.1016/0030-5073(78)90044-2>.
108. Limba T.; Agafonov K., 2012. Elektroninių rinkimų sistemų konstravimo principai, modeliai ir jų apsaugos užtikrinimas. Socialinės technologijos, ISSN 2029-7564.
109. Limba T.; Agafonov K., 2013. Socialinio marketingo technologijų taikymo galimybės elektroninės valdžios paslaugų viešinimui, <https://www.mruni.eu/upload/iblock/540/003_Limba_Agafonov.pdf>.

110. Limba T.; Agafonov K.; Damkus M. 2016. Cyber Security: From Technology to Management, Social Innovations: Theoretical and Practical Insights, 16th International Interdisciplinary Conference on Social Innovations, September 2016, Vilnius, Lithuania.
111. Limba, T.; Agafonov, K.; Paukštė, L.; Damkus, M.; Plėta, T. 2017. Peculiarities of cyber security management in the process of internet voting implementation, Entrepreneurship and Sustainability Issues 5(2): 368-402, <https://doi.org/10.9770/jesi.2017.5.2(15)>.
112. Limba T., Plėta T., Agafonov K., Damkus M., 2017. Cyber security management model for critical infrastructure, Entrepreneurship and Sustainability Issues 4(4): p. 559-573, <http://dx.doi.org/10.9770/jesi.2017.4.4(12)>.
113. Lowrie J., 2015. Cybersecurity: A Primer of U.S. and International Legal Aspects, Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, CRC Press, ISBN-13: 978-1-4822-3923-2.
114. Loukas G.; Gan D.; Vuong T., 2013. A taxonomy of cyber attack and defence mechanisms for emergency management networks, 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), <https://doi.org/10.1109/PerComW.2013.6529554>.
115. Lune H.; Berg B. L., 2017. Qualitative Research Methods for the Social Sciences, 9th edition, Pearson Education, ISBN: 129-2-16439-5.
116. Magklaras G.; Furnell S., 2010. Insider Threat Specification as a Threat Mitigation Technique. Insider Threats in Cyber Security, Springer, <https://link.springer.com/chapter/10.1007/978-1-4419-7133-3_10>.
117. Makura S., 2015. Applying management theory principles in the management of computer information and security, <https://www.researchgate.net/publication/302967563_Applying_management_theory_principles_in_the_management_of_computer_information_and_security?chanel=doi&linkId=5734763b08aea45ee83ac492&showFulltext=true>.
118. Manoochehri G., 1999. The road to manufacturing excellence - Using performance measures to become world-class, Industrial Management (Norcross, Georgia), p. 7-13.
119. Marcinauskaitė R., 2013. Technologinio neutralumo principas ir jo reikšmė formuluojant ir aiškinant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėti, Socialinių mokslų studijos, 2013, 5(1), p. 367–379, ISSN 2029–2244 (online), <https://www3.mruni.eu/ojs/societal-studies/article/download/249/240>.
120. Masero M., 2010. Governance: How to Deal with ICT Security in the Power Infrastructure, <http://dx.doi.org/10.1007/978-90-481-3594-3_6>.
121. Maskell B. H., 1991. Performance measurement for world class manufacturing: a model for American companies, Productivity Press, Cambridge, ISBN-13: 978-0915299997.
122. McNamara D. E., 2009, From Fayol's Mechanistic to Today's Organic Functions of Management, American Journal of Business Education 2(1)2009, <https://files.eric.ed.gov/fulltext/EJ1052767.pdf>.

123. Meyers C.; Powers S.; Faissol D., 2009. Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches, <http://dx.doi.org/10.2172/967712>.
124. Mele D.; Rosanas J., 2003. Power, Freedom and Authority in Management: Mary Parker Follett's „Power-With", Philosophy of Management, 2003, <http://dx.doi.org/10.5840/pom20033221>.
125. Mescon M.H.; Albert M.; Khedouri F., 1985. Management: Individual and Organizational Effectiveness, Harper and Row Publishers, ISBN: 0060444193.
126. Micheli P.; Manzoni J. F., 2010. Strategic performance measurement: Benefits, Limitations and Paradoxes, Long range planning, Vol. 43, Issue 4, p. 463-582, <https://doi.org/10.1016/j.lrp.2009.12.004>.
127. Minchev Z., 2018. Hybrid challenges to human factor in cyberspace.
128. Mishra A.; Gupta B. B.; Gupta D., 2019. Identity Theft, Malware, and Social Engineering in Dealing with Cybercrime, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN-13: 978-0-8153-7133-5.
129. Moschovitis C., 2018. Cybersecurity program development for business, ISBN 9781119430056, JohnWiley & Sons, Inc., Hoboken, New Jersey.
130. Moullin M., 2003. Performance measurement definitions: Linking performance measurement and organisational excellence, <https://doi.org/10.1108/09526860710743327>.
131. Neely A.; Gregory M.; Platts K., 1995. Performance measurement system design: A literature review and research agenda, International Journal of Operations & Production Management, Vol. 15 (4), p. 80-116, <https://doi.org/10.1108/01443579510083622>.
132. O'Neill P. F., 2017. Building Resilience Through Risk Analysis, Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains, Springer, ISBN 97894-024-1126-3.
133. Papadaki E., 2018. What Amendments Need to Be Made to the Current EU Legal Framework to Better Address the Security Obligations of Data Controllers?, PhD Thesys, University of Southampton, Faculty of Physical Sciences and Engineering, School of Electronics and Computer Science, <https://eprints.soton.ac.uk/421046/1/Final_Thesis.pdf>.
134. Papathanasiou A.; Germanos G., 2019. Attacks against information systems in the E.U. environment: legal texts & the joint cybercrime action taskforce (J-CAT) model, Cyber-Security and InformationWarfare, Nova Science Publishers, Inc., ISBN 978-1-53614-385-0.
135. Patiño S.; Yoo S. G., 2018. Study of the Maturity of Information Security in Public Organizations of Ecuador. Technologies and Innovation, 4th International Conference, CITI 2018 Proceedings, Springer, ISBN 978-3-030-00940-3, <https://doi.org/10.1007/978-3-030-00940-3>.
136. Patiño S.; Solís E. F.; Yoo S. G.; Arroyo R., 2018. ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005, 2018 International Conference on eDemocracy & eGovernment (ICEDEG), ISBN 9781538625194, <https://doi.org/10.1109/ICEDEG.2018.8372315>.

137. Prasad P.; Rohokale V., 2020. Cyber Security: The Lifeline of Information and Communication Technology, Springer, ISBN 978-3-030-31702-7.
138. Proença D.; Estevens J.; Vieira R.; Borbinha J., 2017. Risk Management: A Maturity Model Based on ISO 31000, 19th Conference on Business Informatics (CBI) in Thessaloniki, Greece, ISSN: 2378-1971, <https://doi.org/10.1109/CBI.2017.40>.
139. Rainer R. K.; Marshall T. E.; Knapp K. J.; Montgomery G. H., 2007. Do Information Security Professionals and Business Managers View Information Security Issues Differently? Information Systems Security, 16(2), <https://doi.org/10.1080/10658980701260579>.
140. Rao P.; Kamhoua C.; Njilla L.; Kwiat K., 2016. Methods to Detect Cyberthreats on Twitter, Surveillance in Action: Technologies for Civilian, Military and Cyber Surveillance, Springer, ISBN 978-3-319-68532-8, <https://doi.org/10.1007/978-3-319-68533-5>.
141. Rozumski P. K., 2015. The Rise of Social Media and Its Role in Future Protests and Revolutions, Evolution of Cyber Technologies and Operations to 2035, Springer, ISBN 9783-319-23584-4.
142. Sakalas A., 2003. Personalo vadyba, Vilnius, ISBN: 9789986092544.
143. Schultz E. E.; Shumway R.; 2001. Incident Response: A Strategic Guide to Handling System and Network Security Breaches, Sams, ISBN: 1578702569,9781578702565.
144. Schreck T., 2018. IT Security Incident Response: Current State, Emerging Problems, and New Approaches, Doctoral Thesis, <https://opus4.kobv.de/opus4-fau/files/9219/ThomasSchreckDissertation.pdf>.
145. Serpa S.; Ferreira C. M., 2019. The Concept of Bureaucracy by Max Weber, International Journal of Social Science Studies 7(2), <https://dx.doi.org/10.11114/ijsss.v7i2.3979>.
146. Simmons C. B., 2011. Report on the Estonian Internet voting system. Verified Voting Blog, September, <https://www.verifiedvoting.org/report-on-the-estonian-internet-voting-system-2>.
147. Simmons C. B.; Shiva S. G.; Bedi H.; Dasgupta D., 2014. AVOIDIT: A Cyber Attack Taxonomy, 9th Annual Symposium on Information Assurance (ASIA'14), Albany, NY.
148. Shabut A. M.; Lwin K.T.; Hossain M. A., 2016. Cyber attacks, countermeasures, and protection schemes — A state of the art survey. 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), <https://doi.org/10.1109/SKIMA.2016.7916194>.
149. Shamala P.; Ahmad R.; Zolait A.; Sedek M., 2017. Integrating information quality dimensions into information security risk management (ISRM). Journal of Information Security and Applications, < https://doi.org/10.1016/j.jisa.2017.07.004>.
150. Shedden P.; Scheepers R.; Smith W.; Ahmad A., 2011. Incorporating a knowledge perspective into security risk assessments. VINE: The journal of information and knowledge management systems Vol. 41 No. 2, pp.152-166, <https://doi.org/10.1108/03055721111134790>.
151. Singer P.W.; Friedman A., 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know, 2014, ISBN: 0199918112.

152. Solms R.; Niekerk J., 2013. From information security to cyber security, Computers & Security, Vol. 38 (2013), ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2013.04.004>.
153. Solms S. H.; Solms R., 2009. Information security governance, Springer, e-ISBN: 978-0-387-79984-1, <https://doi.org/10.1007/978-0-387-79984-1>.
154. Sofiou S., 2019. Ethics In Cyberspace: Cyber-Security. Cyber-Security and InformationWarfare, Nova Science Publishers, Inc., ISBN 978-1-53614-385-0.
155. Soomro Z. A.; Shah M. H.; Ahmed J., 2016. Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36 (2016).
156. Spencer F. M., 2017. Public-Private Partnerships (PPP)s for Cybersecurity Infrastructures, <https://doi.org/10.13140/RG.2.2.22703.59044>.
157. Springall D.; Finkenauer T.; Durumeric Z.; Kitcat J.; Hursti H.; MacAlpine M.; Halderman J. A., 2014. Security Analysis of the Estonian Internet Voting System.
158. Stankevičius A.; Simanavičienė Ž., 2016. Lobizmo metodų klasifikacijos palyginamoji analizė Lietuvos ir ES teisės aktuose, Visuomenės saugumas ir viešoji tvarka, ISSN 2029-1701, <https://repository.mruni.eu/bitstream/handle/007/15028/Stankevi%C4%8Dius.pdf>.
159. Subrahmanian V.S.; Ovelgönne M.; Dumitras T; Prakash B.A., 2015. The Global Cyber-Vulnerability Report, Springer, ISBN 978-3-319-25758-7.
160. Štitilis D., 2011. Elektroniniai nusikaltimai (mokomasis leidinys). Vilnius, Mykolo Romerio universitetas.
161. Štitilis D., 2013. Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos, Socialinės Technologijos 2013 v. 3(1), ISSN 2029-7564 (online), <https://doi.org/10.13165/ST-13-3-1-13>.
162. Štitilis D.; Klišauskas V., 2015. Aspects of cybersecurity: the case of legal regulation in Lithuania, Journal of Security and Sustainability Issues 5(1), <http://dx.doi.org/10.9770/jssi.2015.5.1(4)>.
163. Štitilis, D.; Pakutinskas, P.; Laurinaitis, M.; Malinauskaitė-van de Castel, I. 2017. A model for the national cyber security strategy. The Lithuanian case, Journal of Security and Sustainability Issues 6(3), <http://dx.doi.org/10.9770/jssi.2017.6.3(3)>.
164. Striteska M.; Jelinkova J., 2014. Strategic Performance Management with Focus on the Customer, 4th International Conference on Leadership, Technology, Innovation and Business Management, p. 77-86, ISBN 978-975-461-514-2.
165. Striteska M.; Jelinkova L. B., 2015. The characteristics of effective performance measurement system: case study analysis, ISBN 978-1-61804-324-5, <http://www.inase.org/library/2015/zakynthos/bypaper/ENG/ENG-47.pdf>.
166. Striteska M.; Spickova M., 2012. Review and Comparison of Performance Measurement Systems, Journal of Organizational Management Studies, Vol. 2012 (2012), <https://ibimapublishing.com/articles/JOMS/2012/114900/114900.pdf>.
167. Ten C.W.; Manimaran G.; Liu C. C., 2010. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. IEEE Transactions on Systems, Man, and

Cybernetics - Part A: Systems and Humans 40(4), <http://dx.doi.org/10.1109/TSMCA.2010.2048028>.
168. Trevors M.; Wallen C. M., 2017. Cyber Hygiene: A Baseline Set of Practices, Software Engineering Institute, Carnegie Mellon University, <https://resources.sei.cmu.edu/asset_files/Presentation/2017_017_001_508771.pdf>.
169. Tisdale S. M., 2015. Cybersecurity: challenges from a systems, complexity, knowledge management and business intelligence perspective, Issues in Information Systems, 16 (2015), <https://doi.org/10.48009/3_iis_2015_191-198>.
170. Trim P.; Lee Y., 2014. Cyber Security Management: A Governance, Risk and Compliance Framework, CRC Press, ISBN 9781472432094.
171. Urbanovič J.; Smalskys V., 2015. Viešojo administravimo mokslo tradicijų raida kontinentinėje Europoje. Viešojo administravimo teorijos, vadovėlis, Vilnius.
172. Ursillo S.; Arnold Ch., 2019. Cybersecurity Is Critical for all Organizations – Large and Small, <https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small>.
173. Urwick L., 1934. The function of administration.
174. Vadiveloo J.; Krutiak J.; Guo J.; Yang J., 2016. Cyber Risk for Small and Medium-Sized Enterprises, The Janet & Mark L. Goldenson Center for Actuarial Research University of Connecticut.
175. Vega R.G.; Arroyo R.; Yoo S.G., 2017. Experience in applying the analysis and risk management methodology called MAGERIT to identify threats and vulnerabilities in an Agro-Industrial Company, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 17, <https://www.ripublication.com/ijaer17/ijaerv12n17_62.pdf>.
176. Vishik C.; Matsubara M.; Plonk A., 2016. Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms, <https://www.ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch11.pdf>.
177. Visuotinė lietuvių enciklopedija (VLE), 2012. Struktūrinis funkcionalizmas. T. XXII (Sko–Šala), Vilnius, Mokslo ir enciklopedijų leidybos institutas.
178. Vlasenko A.; Limba T.; Kiškis M.; Gulevičiūtė G., 2016. Research on Human Emotion while Playing a Computer Game using Pupil Recognition Technology. Journal of the Association for Information Communication Technology Education and Science: p. 417-423, <http://dx.doi.org/10.18421/TEM54-02>.
179. Wei D.; Lu Y.; Jafari M.; Skare P.; Rohde K., 2010. An integrated security system of protecting Smart Grid against cyber attacks, <https://doi.org/10.1109/ISGT.2010.5434767>.
180. Weaver N.; Paxson V.; Staniford S.; Cullingham R., 2003. A taxonomy of computer worms. In Proceedings of the 2003 Workshop on Recurring Malcode, Washington, DC, 2003. ACM Press.
181. Williams K. Y., 2016. Insider-Threat Detection in Corporate Espionage and Cyber-Espionage, National Security and Counterintelligence in the Era of Cyber Espionage, <https://www.igi-global.com/gateway/chapter/141037>.

182. Wolchok S.; Wustrow E.; Isabel D.; Halderman J. A., 2012. Attacking the Washington, D.C. internet voting system. Financial Cryptography and Data Security, Springer, <https://jhalderm.com/pub/papers/dcvoting-fc12.pdf>.
183. Yadav N.; Sagar S.M., 2013. Performance measurement and management frameworks: Research trends of the last two decades, Business Process Management Journal, <http://dx.doi.org/10.1108/BPMJ-01-2013-0003>.
184. Yeo S.; Birch A. S.; Bengtsson H. J., 2015. The Role of State Actors in Cybersecurity: Can State Actors Find Their Role in Cyberspace? Advances in Digital Crime, Forensics, and Cyber Terrorism, ISBN13: 9781466696617.
185. Zakarevičius P., 2002. Vadyba: genezė, dabartis, tendencijos, Kaunas.
186. Zakarevičius P.; Kvedaravičius J.; Augustauskas T., 2004. Organizacijų vystymosi paradigma, Vytauto Didžiojo universitetas, ISBN: 9955120274.
187. Žydžiūnaitė V.; Sabaliauskas S., 2017. Kokybiniai tyrimai. Principai ir metodai, VAGA, ISBN: 978-5-415-02457-5.
188. Воронцов А. В.; Глотов М. Б.; Громов И. А., 2019. История социологии, 2-е изд., ISBN 978-5-534-00629-2.
189. Костенко Е. П.; Михалкина Е. В., 2014. История менеджмента: учебное пособие.; Южный федеральный университет, Ростов-на-Дону.
190. Петухов А. Н.; Гуснин С. Ю., 2019. Эталонная модель безопасности критических информационных инфраструктур. Международная конференция по мягким вычислениям и измерениям.
191. Шелдрейк Дж., 2001. Теория менеджмента: от тейлоризма до японизации. Пер. с англ. под ред. В. А. Спивака, Санкт-Петербург.

Kiti šaltiniai:

192. AbuZaid H., 2015. Enterprise architecture - the family, <https://www.linkedin.com/pulse/enterprise-architecture-family-hamzeh-abuzaid>.
193. ACM TechNews, 2014. States Ditch Electronic Voting Machines, <https://cacm.acm.org/news/180064-states-ditch-electronic-voting-machines/fulltext>.
194. Activtrak.com, 2019. Insider threat detection, <https://activtrak.com/insider-threat-detection>.
195. Barojan D., 2018. Monitoring for Election Interference, Atlantic Council, Digital forensic research lab.
196. Baltic-course, 2016. European human rights court accepts appeal of Estonian e-voting critics, <http://www.baltic-course.com/eng/baltic_states/?doc=115942>.
197. Bayern M., 2019. How a new public-private partnership will fill cybersecurity gaps for the FBI and CIA, <https://www.techrepublic.com/article/how-a-new-public-private-partnership-will-fill-cybersecurity-gaps-for-the-fbi-and-cia>.
198. Baxter A., 2016. The 6 Most Common Social Hacking Exploit Techniques, <https://www.intego.com/mac-security-blog/social-hacking>.
199. Campbell N., 2017. Cyber Security Is A Business Risk, Not Just An IT Problem, <https://www.forbes.com/sites/edelmantechnology/2017/10/11/cyber-security-is-a-business-risk-not-just-an-it-problem/#6a4f34587832>.

200. CERT-UK, 2015. Common Cyber Attacks: Reducing The Impact, Crown Copyright.
201. Chase S., 2018. NATO secretary-general cautions on security threats to 5G network, The Globe and Mail, <https://beta.theglobeandmail.com/politics/article-nato-secretary-general-cautions-on-security-threats-to-5g-network/>.
202. Collier S., 2018. Cybersecurity: It's More than Just Technology, <https://datacenterfrontier.com/cybersecurity-datacenters-technology>.
203. Council of Europe, 2008. The European Critical Infrastructures Directive. Council Directive 2008/114/EC9, <http://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX: 32008L0114>.
204. Cosgrove A., 2019. Human behavior can be your biggest cybersecurity risk, <https://www.helpnetsecurity.com/2019/03/04/human-behavior-cybersecurity-risk/>.
205. Crowdstrike global intelligence team, 2017. Use of Fancy Bear android malware in tracking of Ukrainian Field artillery units.
206. Cybersecurity Enhancement Act (CEA), 2014. U.S. Government Publishing Office, <https://www.gpo.gov/fdsys/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf>.
207. Cybersecurity & Infrastructure Security Agency (CISA), 2009. What is Cybersecurity?, <https://us-cert.cisa.gov/ncas/tips/ST04-001>.
208. Dagienė V.; Grigas G.; Jevsikova T., 2014. Enciklopedinis kompiuterijos žodynas, 4as leidimas, Vilnius.
209. Deighton A., 2015. Cyber security: the dos, the don'ts and the legal issues you need to understand, <https://www.financierworldwide.com/cyber-security-the-dos-the-donts-and-the-legal-issues-you-need-to-understand>.
210. Department of Homeland Security (DHS), 2012. Cybersecurity Questions for CEOs, <https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf>.
211. DNR Digital, 2020. Static vs. Dynamic Cyber Security, <https://dnrdigital.id/static-vs-dynamic-cyber-security>.
212. Donaldson S. E.; Siegel S. G.; Williams C.K.; Aslam A., 2015. Enterprise cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats, Apress, ISBN13: 9781430260837.
213. Dunkelberg D., 2017. The Top 5 Cybersecurity Challenges Facing Financial Service Institutions, <https://www.ispartnersllc.com/blog/top-5-cybersecurity-challenges-facing-financial-service-institutions>.
214. ENISA, 2016. Review of Cyber Hygiene practices, <https://publications.europa.eu/en/publication-detail/-/publication/0918aacc-e922-11e6-ad7c-01aa75ed71a1>.
215. ENISA, 2018. Public Private Partnerships (PPP) - Cooperative models, <https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models>.
216. Ernst & Young LLP (E&Y), 2018. Is the answer to cybersecurity more technology, more people or more process?, <https://www.ey.com/Publication/vwLUAssets/ey-is-the-answer-to-cybersecurity-more-technology-more-people-or-more-

process/$FILE/ey-is-the-answer-to-cybersecurity-more-technology-more-people-or-more-process.pdf>.
217. European Cyber Security Organization (ESCO), 2016. Contractual Public-Private Partnership (cPPP) with the European Commission, <https://ecs-org.eu/cppp>.
218. Federal Office for Information Security (BSI), 2016. The State of IT Security in Germany, <https://www.bsi.bund.de/SharedDocs/Dowloads/EN/BSI/Publications/Securitysituation/ITSecurity-Situation-in-Germany-2016.pdf?__blob=publicationFile&v=3>.
219. Filho A. B., 2005. Computerization of voting in Brazil, <http://cleveland.indymedia.org/news/2006/10/23039.php>.
220. Garcia F. S., 2020. Cooperation and Collaborative Partnerships are Key to Protect Businesses, <https://blog.paloaltonetworks.com/2020/05/network-cooperation>.
221. Garrett A. G., 2018. What CEO's should know & do about cybersecurity, <https://www.bdo.com/getattachment/Insights/Business-Financial-Advisory/What-CEOs-Should-Know-Do-About-Cybersecurity/ADV_Cybersecurity_What-CEOs-should-know-and-do-(2).pdf.aspx>.
222. Giniotienė A., 2019. Kibernetinis saugumas prasideda nuo suvokimo, Verslo žinios, <https://www.vz.lt/verslo-valdymas/2019/11/15/kibernetinis-saugumas-prasideda-nuo-suvokimo>.
223. Haynes K., 2019. Your Security Strategy Is Only as Strong as Your Cyber Hygiene, <https://www.securityintelligence.com/your-security-strategy-is-only-as-strong-as-your-cyber-hygiene>.
224. Huawei Technologies Co. (Huawei), 2019. Huawei's Position Paper on Cyber Security, <https://www-file.huawei.com/-/media/corp/facts/pdf/2019/huaweis-position-paper-on-cyber-security.pdf?la=en>.
225. International telecommunication union (ITU), 2015. Computer incident handling, <https://www.itu.int/en/ITUD/Cybersecurity/Documents/Computer%20Incident%20Handling%20.pdf>.
226. Johansen G., 2017. Digital Forensics and Incident Response: An intelligent way to respond to attacks, Packt, ISBN 978-1-78728-868-3.
227. Johansen A. G., 2020. What is cyber security? What you need to know, <https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html>.
228. James M., 2018. Six Cybersecurity Tools and Services Every Business Needs, <https://www.globalsign.com/en/blog/six-cybersecurity-tools-and-services-every-business-needs/>.
229. Jones D. W., 2003. The case of the Diebold FTP site, <http://homepage.divms.uiowa.edu/~jones/voting/dieboldftp.html>.
230. Jurčenkaitė I., 2019. Pasakyta/Padaryta. „Valstiečiai" išsižada rinkimų pažado įteisinti balsavimą internetu, <https://www.15min.lt/naujiena/aktualu/lietuva/valstieciai-issizada-pazado-iteisinti-elektronini-balsavima-56-1100000>.
231. Institute of Risk Management (IRM), 2018. A Risk Practitioners Guide to ISO 31000:2018, <https://theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf>.

232. International Information System Security Certification Consortium (ISC)2, 2015. Common Body of Knowledge (CBK), 4th edition, ed. Gordon A.
233. International Organization for Standardization (ISO); International Electro Technical Commission (IEC), 2013. Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002:2013).
234. International Organization for Standardization (ISO), 2012. Information technology — Security techniques — Guidelines for cybersecurity (ISO 27032:2012).
235. International Organization for Standardization (ISO), 2018. Risk Management – Guidelines (ISO 31000:2018).
236. Kaspersky Lab, 2020, What is Cyber Security?, <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>.
237. Kenton W, 2018. Gator, <https://www.investopedia.com/terms/g/gator.asp>.
238. KPMG International, 2016. Cyber security: a failure of imagination by CEOs, <https://assets.kpmg/content/dam/kpmg/pdf/2016/02/cyber-ceo-report.pdf>.
239. Krauel S.; Bay S., 2018. Understanding hybrid threats, Hybrid Threats and Digital Landscape, Vilnius.
240. Lardy B., 2020. How one public-private partnership is closing the cybersecurity talent gap, <https://ourpublicservice.org/blog/how-one-public-private-partnership-is-closing-the-cybersecurity-talent-gap>.
241. Latham & Watkins, 2016. 5 Preventative Steps to Manage Legal Risk Following a Cybersecurity Breach, <https://www.lw.com/thoughtLeadership/5-preventative-steps-to-manage-legal-risk-following-a-cybersecurity-breach>.
242. Lietuvos standartizacijos departamentas (LST), 2011. Informacinės technologijos. Saugumo metodai. Informacijos saugumo rizikos valdymas, LST ISO/IEC 27005.
243. Lietuvos standartizacijos departamentas (LST), 2014. Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo priemonių praktikos nuostatai, LST ISO/IEC 27002.
244. Lipma H., 2011. Paper-voted (and why I did so), <https://helger.wordpress.com/2011/03/05/paper-voted-and-why-i-did-so>.
245. Maurer T.; Morgus R., 2014. Compilation of Existing Cybersecurity and Information Security Related Definitions, <https://www.newamerica.org/cybersecurity-initiative/policy-papers/compilation-of-existing-cybersecurity-and-information-security-related-definitions>.
246. Marine D., 2018. Security Incidents: Incident Handling vs Incident Response, eLearnSecurity, <https://elearnsecurity.com/security-incidents-incident-handling-vs-incident-response.html>.
247. Meltzer J. P., 2020. Cybersecurity, digital trade, and data flows: Re-thinking a role for international trade rules, <https://www.brookings.edu/wp-content/uploads/2019/11/Cybersecurity-digital-trade-data-flows.pdf>.
248. Miller J., 2019. What is Security Incident Response Plan?, <https://www.bitlyft.com/what-is-security-incident-response-plan-2>.
249. Mukherjee D., 2020. Threat Detection has Evolved from Static to Dynamic Behavioral Analysis to Detect-Threatening Behavior, CISO MAG, <https://cisomag.

eccouncil.org/threat-detection-has-evolved-from-static-to-dynamic-behavioral-analysis-to-detect-threatening-behavior>.
250. Nacionalinis kibernetinio saugumo centras (NKSC), 2018. NKSC veikla, <https://www.nksc.lt/veikla.html>.
251. National Institute of Standards and Technology (NIST), 2012. Computer Security Incident Handling Guide, <http://dx.doi.org/10.6028/NIST.SP.800-61r2>.
252. National Institute of Standards and Technology (NIST), 2018. Framework for Improving Critical Infrastructure Cybersecurity v1.1, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
253. NATO Cooperative Cyber Defence Center Of Excellence, (NATO CCDCOE), 2015. Cyber definitions, <https://ccdcoe.org/cyber-definitions.html>.
254. NATO Cooperative Cyber Defence Centre of Excellence, 2016. Tallinn manual 2.0 on the international law applicable to cyber operations, ISBN 9781107177222.
255. news.err.ee, 2013. Center Party Petitions European Human Rights Court Over E-Voting, <https://news.err.ee/108344/center-party-petitions-european-human-rights-court-over-e-voting>.
256. North Atlantic Treaty Organization (NATO), 2010. Active engagement, Modern Defence, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, adopted by Heads of State and Government at the NATO Summit in Lisbon, <http://www.nato.int/cps/po/natohq/official_texts_68580.htm>.
257. NSW Electoral Commission, 2014. iVote threat analysis and risk assessment – SGE 2015, <http://www.elections.nsw.gov.au/__data/assets/pdf_file/0008/175760/NSW_Election_-_iVote_Threat_Analysis_and_Risk_Assessment_v3.0.pdf>.
258. Oltsik J., 2016. Cybersecurity, business and IT relationships, <https://www.csoonline.com/article/3133954/cybersecurity-business-and-it-relationships.html>.
259. Petters J., 2018. What is Incident Response? A 6-Step Plan, Varonis, <https://www.varonis.com/blog/incident-response-plan/>.
260. Petryni M., 2019. The Importance of Human Relations in the Workplace, <https://smallbusiness.chron.com/advantages-disadvantages-having-diverse-workforce-22935.html>.
261. Radar First, 2020. Privacy Incident Response – A Repetitive Yet Unique Process, <https://www.radarfirst.com/blog/privacy-incident-response-a-repetitive-yet-unique-process>.
262. Reddy N., 2019. Practical Cyber Forensics, Apress, ISBN-13 (electronic): 978-1-4842-4460-9, <https://doi.org/10.1007/978-1-4842-4460-9_1>.
263. Riddle J., 2019. What's the Role of HR in Cybersecurity and Why Is It Important?, <https://blog.devolutions.net/2019/07/whats-the-role-of-hr-in-cybersecurity-and-why-is-it-important>.
264. Salinas S., 2018. Six top US intelligence chiefs caution against buying Huawei phones, <https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html>.
265. SANS Institute, 2018. CIS Controls v.7, <http://www.defensis.it/ecms/file/CIS-Controls-Version-7.pdf>.

266. Sheymov V., 2016. What is Cyberspace?, <https://victorsheymov.com/what-is-cyberspace>.
267. Singh M., 2017. Five reasons why enterprise leaders should be looking at Dynamic Cybersecurity, HCL Technologies, <https://www.hcltech.com/blogs/five-reasons-why-business-and-it-leaders-should-be-looking-dynamic-cybersecurity>.
268. Singh M., 2018. Cybersecurity: Move From Static To Dynamic Posture To Future Secure Yourself, ERP Insight, <http://www.theerpinsights.com/insight/cybersecurity-move-from-static-to-dynamic-posture-to-future-secure-yourself-fid-276.html>.
269. SiliconRepublic.com, 2006. E-voting machines successfully hacked. <http://www.siliconrepublic.com/news/news.nv?storyid=single7158>.
270. Šarkūnas A., 2017. Kibernetinį saugumą palygino su meteorologija: niekada nežinai, kokia audra gali ateiti, LRT.lt, <https://www.lrt.lt/naujienos/lietuvoje/2/186860/kibernetini-sauguma-palygino-su-meteorologija-niekada-nezinai-kokia-audra-gali-ateiti>.
271. The Economist, 2010. Cyberwar: War in the fifth domain, <https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain>.
272. United States Department of Energy, 2006. Roadmap to Secure Control Systems in the Energy Sector.
273. US-CERT, 2016. Cyber Resilience Review (CRR): NIST Cybersecurity Framework Crosswalks, Department of Homeland Security, <https://www.us-cert.gov/ccubedvp/assessments#Downloadable Resources>.
274. Shkedi A., 2019. Introduction to Data Analysis in Qualitative Research: Practical and theoretical Methodologies with optional use of a software tool.
275. Statista.com, 2018. Global number of cyber security incidents from 2009 to 2015 (in millions), <https://www.statista.com/statistics/387857/number-cyber-security-incidents-worldwide>.
276. Stichting Wij Vertrouwen Stemcomputers Niet, 2008. The Netherlands return to paper ballots and red pencils, <http://wijvertrouwenstemcomputersniet.nl/English>.
277. StratCom Centre of Excellence (NATO StratCom COE), 2018. Defence against Election Interference, Hybrid Threats and Digital Landscape, Vilnius.
278. StratCom Centre of Excellence (NATO StratCom COE), 2018. Disinformation/Fake news, Hybrid Threats and Digital Landscape, Vilnius.
279. Superior Electoral Court, 2014. Learn about the history of Brazilian electronic voting machines, which goes back 18 years, <http://english.tse.jus.br/noticias-tse-en/2014/Julho/learn-about-the-history-of-brazilian-electronic-voting-machines-which-goes-back-18-years>.
280. Superior Electoral Court, 2018. 4 days left for the General Elections of 2018: get to know the voting order on the Electronic Voting Machine (EVM) for the 2018 Elections, <http://english.tse.jus.br/noticias-tse-en/2018/Outubro/4-days-left-for-the-general-elections-of-2018-get-to-know-the-voting-order-on-the-electronic-voting-machine-evm-for-the-2018-elections>.
281. Techrepublic, 2004. Disaster Planning and Recovery Pack.

282. United States Government Accountability Office (GAO), 2005. Department of Homeland Security›s (DHS›s) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO05434, Washington.
283. United States Government Accountability Office (GAO), 2007. Critical Infrastructure Protection - Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain, <http://www.gao.gov/assets/270/268137.pdf>.
284. Volz D., 2016. U.S. government concludes cyber attack caused Ukraine power outage, <http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K>.
285. Valstybės saugumo departamentas (VSD), Antrasis opertyvinių tarnybų departamentas prie krašto apsaugos ministerijos (AOTD), 2019. Grėsmių nacionaliniam saugumui vertinimas, <https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-LT.pdf>.
286. Vyriausioji rinkimų komisija (VRK), 2018. Apie Vyriausiąją rinkimų komisiją, <https://www.vrk.lt/vrk-apie>.
287. Walker S., 2018. Cybersecurity Guidelines, International BAR Association, <www.ibanet.org/LPRU/LPRU-Cybersecurity.aspx>.
288. Water Information Sharing and Analysis Center (WISAC), 2015. 10 Basic Cybersecurity Measures Best Practices to Reduce Exploitable Weaknesses and Attacks, <https://icscert.uscert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf>.
289. Zhao J., 2020. How to Create a Cybersecurity Incident Response Plan, <https://hyperproof.io/resource/cybersecurity-incident-response-plan>.
290. Zorz Z., 2020. Building relationships: The key to becoming a true cybersecurity leader, <https://www.helpnetsecurity.com/2020/06/18/cybersecurity-building-relationships/>.

PRIEDAI

1 PRIEDAS

Kibernetinio saugumo valdymo modelio empirinio tyrimo klausimynas.

Gerbiamas eksperte, nuoširdžiai dėkoju Jums, kad sutikote dalyvauti mano atliekamame tyrime. Tyrimas organizuojamas rengiant daktaro disertaciją tema „Kibernetinio saugumo valdymo modelis elektroninių rinkimų įgyvendinimui“. Empirinio tyrimo metu surinkta informacija, neatskleidžiant respondentų tapatybės, bus apibendrinta ir paskelbta rengiamoje disertacijoje.

Tyrimo tikslas – išsiaiškinti konceptualaus kibernetinio saugumo valdymo modelio gyvybiškumą ir tinkamumą elektroninių rinkimų įgyvendinimui, o taip pat patikslinti konceptualaus modelio struktūrą, atsižvelgiant į tyrimo metu gautus respondentų atsakymus.

Empirinis tyrimas yra suskirstytas į 3 logines dalis:

- Pirmiausia Jums bus pateiktas klausimas apie kibernetinį saugumą, siekiant išsiaiškinti jūsų nuomonę kaip turi būti suprantamas kibernetinis saugumas dabartiniame pasaulyje.
- Antroje dalyje jums bus pateikti klausimai susiję su konceptualaus kibernetinio saugumo valdymo modelio dimensijų validavimu. Konceptualaus kibernetinio saugumo valdymo modelio struktūrinė schema yra pavaizduota 1 paveiksle, kuriame yra pateiktos šešios kibernetinio saugumo valdymo dimensijos: Organizacijos valdymo procesų, Teisinio reguliavimo, Kibernetinio saugumo kultūros, Technologinio kibernetinio saugumo, Rizikos valdymo, Kibernetinių incidentų valdymo. Šios kibernetinio saugumo valdymo dimensijos buvo identifikuotos vykdant teorinius tyrimus ir atliekant egzistuojančių kibernetinio saugumo valdymo modelių (SUNS, NIST, $(ISC)^2$, ISO27001/27002) lyginamąją analizę. Prieš kiekvieną klausimą bus pateikiama bendra trumpa informacija apie kiekvieną modelio dimensiją.
- Trečioje dalyje Jūsų bus prašoma pateikti savo nuomonę apie Kibernetinio saugumo valdymo modelio pritaikomumą Lietuvos elektroninių rinkimų sistemos kūrimui.

Dėkoju už Jūsų pagalbą.
Konstantin Agafonov

1 paveikslas. *Kibernetinio saugumo valdymo modelis*

1 klausimas:

Kaip jus suprantate kibernetinį saugumą?

2 klausimas:

Organizacijos valdymo procesų dimensija yra susieta su trumpalaikiais ir ilgalaikiais organizacijos tikslais, organizacijos veiklos strategija, valdymu bei vadovavimu organizacijai.

Organizacijos valdymo procesai
Kokia yra kibernetinio saugumo valdymo reiškinio įtaką organizacijos valdymo procesų dimensijai?
Ar kibernetinio saugumo valdymo reiškinio suvokimas (supratimas) ir naudojimas organizacijoje, jos valdymo sistemoje bei tarp organizacijos narių įtakoją pačios organizacijos kibernetinio saugumo užtikrinimo procesą?
Kaip kibernetinis saugumas turi būti suprantamas organizacijos kasdieniame gyvenime ir jos vykdomoje veikloje?

Organizacijos valdymo procesai
Kokia yra kibernetinio saugumo dedamosios reikšmė organizacijos vykdomose (naujai įgyvendinamose) projektuose ir kaip gali būti tobulinamas kibernetinio saugumo dedamosios įtraukimas į organizacijos vykdomą veiklą? Ar siekiant kibernetinio saugumo užtikrinimo įgyvendinimo organizacijoje yra būtina atlikti organizacijos valdymo procesų peržiūrą ir koregavimą? Kokių veiksmų privalo imtis organizacija, siekdama patobulinti savo valdymo procesus kibernetinio saugumo reiškinio kontekste: • Organizacijos siekiamų tikslų identifikavimas; • Organizacijos veiklos pokyčių identifikavimas; • Organizacijos aplinkos ypatumų nustatymas; • Kibernetinio saugumo reiškinio integravimas į organizacijos veiklos procesus; • Kiti veiksmai.

3 klausimas:

Kibernetinio saugumo valdymo modelio **teisinio reguliavimo dimensija** yra siejama su organizacijoje vykstančiais bei jai įtaką darančiais teisinio reglamentavimo procesais.

Teisinis reguliavimas
Kokios priežastys lemia būtinybę nagrinėti teisinio reguliavimo organizacijoje sritį kibernetinio saugumo kontekste? Ar teisinio reguliavimo procesai gali įtakoti kibernetinį saugumą organizacijoje? Ar nagrinėjant organizacijos kibernetinio saugumo valdymo įgyvendinimo kontekstą būtina atsižvelgti į vidinės ir išorinės aplinkos teisinio reguliavimo poveikį organizacijai? Kokia organizacijos aplinką (išorinė ar vidinė) nagrinėjant jas kibernetinio saugumo teisinio reguliavimo kontekste yra svarbesnė? Kaip turi būti įgyvendinamas teisinis reguliavimas organizacijoje ir kokių veiksmų privalo imtis organizacija, siekdama patobulinti teisinio reguliavimo aspektus kibernetinio saugumo reiškinio kontekste: • Esamos teisinio reglamentavimo sistemos reikalavimų ir trūkumų nustatymas; • Trūkumų šalinimo priemonių įgyvendinimas; • Įgyvendintų priemonių taikymo ir organizacijos veikloje auditavimas; • Teisinio reguliavimo priemonių integravimas į organizacijos veiklos procesus; • Kiti veiksmai.

4 klausimas:

Kibernetinio saugumo kultūros dimensija yra glaudžiai susijusi su žmogiškojo faktoriaus įtaka kibernetinio saugumo valdymo procesui organizacijoje.

Kibernetinio saugumo kultūra
Kokia yra pagrindinė kibernetinio saugumo kultūros problema organizacijos kibernetinio saugumo valdymo kontekste ir kokie galimi jos sprendimo būdai? Ar organizacijos kibernetinio saugumo kultūros aspektai turi būti taikomi ir organizacijos partneriams bei organizacijai paslaugas teikiantiems partneriams? Kokių veiksmų būtina imtis organizacijoje sprendžiant žmogiškojo faktoriaus įtakos ir kibernetinio saugumo kultūros reiškinio problemas organizacijoje: • Identifikuoti kibernetinio saugumo suvokimo problematiką; • Numatyti kibernetinio saugumo suvokimo gerinimo metodus ir budus; • Atlikti kibernetinio saugumo kultūros pokyčių stebėjimą; • Kiti veiksmai.

5 klausimas:

Technologinis kibernetinis saugumas dažniausiai siejamas su techninėmis ir programinėmis priemonėmis naudojamomis kibernetinio saugumo užtikrinimui.

Technologinis kibernetinis saugumas
Kokios dar technologinio kibernetinio saugumo įgyvendinimo priemonės yra svarbios, siekiant užtikrinti technologinį kibernetinį saugumą organizacijoje? Ar organizacijai yra būtina vadovautis tam tikromis technologinių priemonių valdymo standartais ar rekomendacijomis, siekiant darnaus technologinio kibernetinio saugumo vystymo? Ar technologinio kibernetinio saugumo valdymo priemonės turi turėti technologinį neutralumą? Nuo ko turi priklausyti technologinio kibernetinio saugumo užtikrinimo priemonių parinkimas organizacijoje? Kokius veiksmus privalo atlikti organizacija siekiant užtikrinti tinkamą technologinio kibernetinio saugumo įgyvendinimą: • Naudojamų technologinių priemonių identifikavimas; • Technologinių priemonių parinkimas ir įdiegimas; • Technologinių priemonių panaudojimo įtakos kibernetiniam saugumui vertinimas; • Kiti veiksmai.

6 klausimas:

Organizacijos **rizikos valdymo dimensija** yra siejama su organizacijos galimybėmis tinkamai identifikuoti, valdyti ir prisiimti jai iškylančias ir įtaką darančias vidines ir išorines organizaciją supančių aplinkų rizikas.

Rizikos valdymas
Ar rizikos valdymo procesas yra svarbus organizacijai kibernetinio saugumo užtikrinimo kontekste? Ar kibernetinio saugumo valdymas organizacijoje gali būti vykdomas neatsižvelgiant į rizikos valdymo aspektus? Kokių veiksmų turi imtis organizacija siekiant tinkamai įgyvendinti rizikos valdymo procesus: • Identifikuoti rizikos valdymo procesus organizacijoje; • Suklasifikuoti galimas rizikas bei atlikti jų vertinimą; • Parengti rizikos valdymo planus ir taisykles; • Kiti veiksmai.

7 klausimas:

Kibernetinių incidentų valdymo dimensija yra siejama su organizacijos galimybėmis aptikti, suvaldyti bei efektyviai priešintis atsirandantiems ar vykstantiems kibernetiniams incidentams.

Kibernetinių incidentų valdymas
Koks požiūris į kibernetinių incidentų valdymą yra labiau priimtinas šiuolaikiniame pasaulyje: atsako į kibernetinius incidentus (*angl. incident response*) ar kibernetinių incidentų valdymo (*angl. incident handling*)? Kokie šių požiūrių privalumai ar trūkumai gali būti identifikuojami kibernetinio saugumo valdymo organizacijoje kontekste? Ar siekiant visapusiško kibernetinio saugumo organizacijoje šie požiūriai į kibernetinių incidentų valdymą turi būti nagrinėjami neatsiejamai vienas nuo kito? Kokių veiksmų turi imtis organizacija siekiant tinkamai įgyvendinti kibernetinių incidentų valdymą: • Reglamentuoti kibernetinių incidentų valdymo etapus; • Parengti organizacijos veiklos planus; • Atlikti įvykusių incidentų tyrimus, nustatant jų atsiradimo priežastis; • Kiti veiksmai.

8 klausimas:

Jūsų nuomone:

1. ar tyrimo metu pristatytas kibernetinio saugumo valdymo modelis gali būti naudojamas įgyvendinant elektroninius rinkimus Lietuvoje?
2. kokios organizacijos, institucijos galėtų dalyvauti ar būti atsakingos įgyvendinant elektroninius rinkimus?

9 klausimas:

1. Ar turėtumėte papildomų pastabų ir pasiūlymų?

MYKOLO ROMERIO UNIVERSITETAS

Konstantin Agafonov

KIBERNETINIO SAUGUMO VALDYMO MODELIS ELEKTRONINIAMS RINKIMAMS ĮGYVENDINTI

Daktaro disertacijos santrauka
Socialiniai mokslai, vadyba (S 003)

Vilnius, 2021

Mokslo daktaro disertacija rengta 2015–2021 metais Mykolo Romerio universitete pagal Vytauto Didžiojo universitetui su Klaipėdos universitetu, Mykolo Romerio universitetu ir Šiaulių universitetu Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2019 m. vasario 22 d. įsakymu Nr. V-160 suteiktą doktorantūros teisę.

Mokslinis vadovas:
prof. dr. Tadas Limba (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, S 003).

Mokslo daktaro disertacija ginama Vytauto Didžiojo universiteto, Klaipėdos universiteto, Mykolo Romerio universiteto ir Vilniaus universiteto Šiaulių akademijos vadybos mokslo krypties taryboje:

Pirmininkė:
prof. dr. Rima Žitkienė (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, S 003).

Nariai:
prof. dr. Vida Davidavičienė (Vilniaus Gedimino technikos universitetas, socialiniai mokslai, vadyba, S 003);
prof. dr. Fernando Galindo (Saragosos universitetas, Ispanijos Karalystė, socialiniai mokslai, teisė, S 001);
prof. dr. Rimantas Stašys (Klaipėdos universitetas, socialiniai mokslai, vadyba, S 003);
prof. dr. Diana Šaparnienė (Vilniaus universiteto Šiaulių akademija, socialiniai mokslai, vadyba, S 003).

Daktaro disertacija bus ginama viešame Vadybos mokslo krypties tarybos posėdyje 2021 m. spalio 7 d. 11 val. Mykolo Romerio universitete, I-414 auditorijoje.
Adresas: Ateities g. 20, Vilnius.

Daktaro disertacijos santrauka išsiųsta 2021 m. rugsėjo 7 d.

Daktaro disertaciją galima peržiūrėti Lietuvos nacionalinėje Martyno Mažvydo bibliotekoje (Gedimino pr. 51, Vilnius), Klaipėdos universiteto (K. Donelaičio a. 3, Klaipėda), Mykolo Romerio universiteto (Ateities g. 20, Vilnius), Vilniaus universiteto Šiaulių akademijos (Vytauto g. 84, Šiauliai), Vytauto Didžiojo universiteto (K. Donelaičio g. 52, Kaunas) bibliotekose.

Konstantin Agafonov

KIBERNETINIO SAUGUMO VALDYMO MODELIS ELEKTRONINIAMS RINKIMAMS ĮGYVENDINTI

SANTRAUKA

Temos aktualumas. Šiuolaikinė visuomenė, jos gyvenimas ir socialiniai santykiai yra stipriai priklausomi nuo kibernetinės erdvės, todėl pasaulio informacinių technologijų specialistai ir įvairių mokslo krypčių atstovai deda dideles pastangas kibernetinio saugumo problemoms spręsti. Yra sukurtos ir plačiai taikomos informacijos saugumo valdymo technologijos, standartai, tačiau jie yra labiau susiję su informacijos saugumo ir technologijų valdymu organizacijos viduje, tuo tarpu kibernetinio saugumo valdymas apima ne tik vidinių grėsmių ir kibernetinio saugumo technologijų valdymą, bet ir galimų rizikų bei išorinių grėsmių stebėjimą, atsako į grėsmes galimybių bei grėsmių išvengimo priemonių vertinimą, personalo mokymą ir kibernetinio saugumo teisinį reguliavimą. Kompiuterinės sistemos ir technologiniai sprendimai, naudojami privataus sektoriaus veiklai organizuoti ir pertvarkyti, dabartiniais laikais plačiai pritaikomi ir viešajame sektoriuje. Valstybės ir piliečių nuolatinis bendravimas yra etapais perkeliamas į skaitmeninę erdvę. Toks perkėlimas sąlygoja greitesnį viešųjų paslaugų suteikimą piliečiams bei mažina viešojo administravimo institucijų veiklos krūvį. Technologinė revoliucija taip pat lemia bandymus naudoti šiuolaikines informacines ir telekomunikacines technologijas pasaulio valstybių politiniuose procesuose. Valstybės, naudodamos technologijas, bando priartinti piliečius prie šalies valdymo ir tiesioginio dalyvavimo įvairiuose šalyje vykstančiuose politiniuose procesuose, o vienas iš dažniausiai naudojamų politinio dalyvavimo ir gyventojų įtraukimo į politinius procesus įrankis yra elektroninis balsavimas.

Šiuolaikinis pasaulis pasiekė labai aukštą technologinį išsivystymo lygį, tačiau jis vis dar nėra saugus kibernetinio saugumo prasme: pastebimas tendencingas kibernetinių saugumo incidentų skaičiaus augimas, kibernetinių nusikaltėlių naudojamos įsibrovimų technologijos tampa sudėtingesnės ir vis sunkiau aptinkamos (Simmons ir kt., 2014), o tradiciniai technologiniai kibernetinio saugumo užtikrinimo įrankiai nėra pajėgūs atpažinti ir sustabdyti visas piktavalių rengiamas kibernetines atakas (Shabut ir kt., 2016). Yra atlikta nemažai mokslinių tyrimų, kurie yra susiję su informacijos saugumo valdymu organizacijose: informacijos saugumas nagrinėjamas atskirose mokslo srityse ne tik techniniu, bet ir vadybos, ekonomikos ir kitų mokslų kontekste (Ashenden, 2008; Bakshi ir kt., 2009; Jastiuginas, 2011; Johnson, 2015), tačiau to nepakanka, kad būtų galima sukurti kibernetinio saugumo valdymo modelį, kuris aiškiai ir vienareikšmiškai nusakytų kibernetinio saugumo valdymo aspektus, kuriant valstybės informacines sistemas ir teikiant elektronines paslaugas gyventojams. Nors ir nėra sukurtas bendras kibernetinio saugumo valdymo modelis, visos pasaulio valstybės supranta, kad yra būtina valdyti ir kruopščiai apsaugoti savo informacinius išteklius,

o mokslininkai yra pažymėję, kad šalies ypatingos svarbos (kritinės) infrastruktūros saugumas yra būtinas ir turi būti valdomas kompleksiškai (Limba ir kt., 2017; NATO StratCom COE, 2018; Haynes, 2019; Giniotienė 2019; Sofiou, 2019).

Kibernetinio saugumo reiškinys yra nagrinėjamas nuo dvidešimtojo amžiaus paskutiniojo dešimtmečio. Pastebėtina, kad šios sąvokos esmė ir turinys kito nuo jos atsiradimo, o šis pasikeitimas yra siejamas su technologinių sistemų tobulėjimu ir kaita. Kibernetinio saugumo (informacijos saugumo) reiškinys buvo pradėtas nagrinėti telekomunikacinių ir kompiuterinių sistemų apdorojamos informacijos saugumo kontekste, vėliau – kompiuterinėse sistemose perduodamos informacijos saugumo kontekste ir, galiausiai, informacijos vientisumo, prieinamumo, autentiškumo, patikimumo ir konfidencialumo užtikrinimo kontekstuose.

Viešojo sektoriaus atstovai, politikai, mokslininkai ir technologijų saugumo ekspertai sutaria, kad vien technologinių klausimų sprendimai nepanaikina visų problemų tol, kol nėra sukurtas kibernetinio saugumo valdymo modelis, taikytinas elektroniniams rinkimams įgyvendinti. Iš esmės problema slypi tame, kad kibernetinis saugumas turi būti traktuojamas ne tik kaip techninė disciplina ar pasiekiamas techninis lygis (Lowrie, 2015), bet kaip organizacijos valdymo koncepcija (Rainer ir kt., 2007). Koncepcija kurioje maksimaliai yra agreguojamos visos įmanomos priemonės: techninės, teisinės (Štitilis ir kt., 2017), o svarbiausia – vadybos strategijos ir pasiekiama tam tikra organizacijos branda (Lackram, Padayachee, 2018; Patiño, Yoo, 2018).

Kibernetinio saugumo valdymo problema elektroninių rinkimų įgyvendinimo kontekste pasaulyje yra mažai atskleista, bet aktuali. 2014 m. Jungtinės Tautos pradėjo pasaulinį kibernetinio saugumo stebėjimo projektą, kuris turėtų užtikrinti saugumo, žmogaus teisių stebėjimo bei ekonominių ir geruųjų valdymo praktikų įgyvendinimą. Šiuo disertaciniu darbu siekiama sukurti kibernetinio saugumo valdymo modelį, kuris gali būti pritaikytas, kuriant ir valdant kibernetinį saugumą elektroninių rinkimų sistemose. Elektroninių rinkimų įgyvendinimas yra vienas iš pagrindinių būdų skatinti piliečių dalyvavimą šalies politiniuose procesuose, o didžiausias šių sistemų trūkumas – sistemų saugumo stoka. Tikėtina, kad kibernetinio saugumo valdymo modelis, kuris bus kuriamas ir nagrinėjamas disertacijoje, pagreitins elektroninių rinkimų įgyvendinimą ir paspartins elektroninių rinkimų pripažinimą.

Temos ištirtumo lygis. Pasaulio mokslininkai, tarptautinės organizacijos ir kibernetinio saugumo technologinės ir programinės įrangos gamintojai kibernetinio saugumo valdymą nagrinėja įvairiais aspektais.

Mokslinėje literatūroje vis dar kyla diskusijos dėl paties kibernetinio saugumo reiškinio apibūdinimo. Kibernetinio saugumo reiškinį, jo kaitą ir esmę nagrinėjo Anderson, 2001; Ashenden, 2008; Jastiuginas, 2011; Agrawal, Campoe, Pierce, 2014; Alotaibi, Furnell, Clarke, 2016; Dykstra, 2017; Limba, Plėta, Agafonov, Damkus, 2017; Grincevičius, 2018 ir kiti pasaulio mokslininkai.

Autoriai Landwehr, Bull, McDermott, Choi, 1994; Howard, Longstaff, 1998; Weaver, Paxson, Staniford, Cullingham, 2003; Hansman, Hunt, 2003; Kjaerland, 2006; Gruschka, Jensen, 2010; Štitilis, 2011; Limba, Agafonov, 2012; Simmons, Shiva, Bedi, Dasgupta, 2014; Shabut, Lwin, Hossain, 2016 ir kiti mokslininkai rašo apie kiberneti-

nio saugumo incidentų ir atakų klasifikavimo sistemas, identifikuoja galimus jų atlikimo būdus ir metodus.

Pasaulio mokslininkai taip pat nagrinėja kibernetinį saugumą teisiniais aspektais: Štitilis, 2013; Appazov, 2014; Lowrie, 2015; Deighton, 2015; Štitilis, Klišauskas, 2015; Kosseff, 2018, rizikos valdymo aspektais: Kroger, 2008; Ackermann, 2012; Agrawal, 2014; Chen, Pedrycz, Ma, Wang, 2014; Deighton, 2015; Proença, Estevens, Vieira, Borbinha, 2017; Vega, Arroyo, Yoo, 2017; Walker, 2018; Grincevičius, 2018; Patiño, Solís, Yoo, Arroyo, 2018, technologinio saugumo aspektais: Cayirci, Ghergherehchi, 2011; Solms, Niekerk, 2013; Donaldson, Siegel, Williams, Aslam, 2015; Alotaibi, Furnell, Clarke, 2016; Campbell, 2017; Collier, 2018, incidentų valdymo aspektais: Deighton, 2015; Beissel, 2016; Craig, Valeriano, 2016; Limba, Agafonov, 2012; procesų valdymo ir kontrolės aspektais: Rainer, Marshall, Knapp, Montgomery, 2007; Solms, 2009; Deighton, 2015; Latham&Watkins, 2016; Limba, Agafonov, Paukštė, Damkus, Plėta, 2017; Moschovitis, 2018; Patiño, Yoo, 2018, bei socialiniais ir kitais aspektais.

Kibernetinių incidentų atsiradimo ypatumus ir priežastis analizuoja Andersen, 2001; Barnes, Johnson, Nickelson, 2004; Masero, 2010; Wei, 2010; Cayirci, Ghergherehchi, 2011; Singer, Friedman, 2014; Craig, Valeriano, 2016; Voltz, 2016; Limba, Plėta, Agafonov, Damkus, 2017; Govindarasu, Hanas, 2017 ir kiti mokslininkai bei įvairios viešojo ir privataus sektoriaus organizacijos: ISO/IEC, 2013; USCERT, 2018; $(ISC)^2$, 2015; SANS, 2018 ir kt., kurios, siekdamos užtikrinti kibernetinio saugumo valdymą organizacijose, per pastaruosius du dešimtmečius sukūrė sistemas ir standartus, kurie gali būti naudojami, kuriant kibernetinį saugumą.

Elektronines rinkimų sistemas, jų veikimo principus, teorinius bei realius elektroninių balsavimo sistemų pažeidžiamumus ir jų atsiradimo priežastis nagrinėjo Jefferson, Rubin, Simons, Wagner, 2004; Kohno, Stubblefield, Rubin, Wallach, 2004; Filho, 2005; Fieldman, Halderman, Felten, 2006; Hursti, 2006; Gonggrijp, Hengeveld, 2007; Simmons, 2011; Limba, Agafonov, 2012; Chowdhury, 2013; Aranha, Karam, Miranda, Scarel, 2014; Brightwell, Cucurull, Galindo, Guasch, 2015; Karda, Kiraz, Bingöl, Birinci, 2016; Goldsmith, 2017; Halderman, 2017; Limba, Agafonov, Paukštė, Damkus, Plėta, 2017; Augoye, Tomlinson, 2018 ir kt., ypatingą dėmesį skirdami kibernetinių incidentų atsiradimo priežasčių nustatymui, taip siekdami identifikuoti esminius faktorius, darančius įtaką elektroninių rinkimų sistemų panaudojimui demokratiniuose procesuose.

Pažymėtina, kad, nors kibernetinis saugumas įvairiausiais aspektais yra pakankamai plačiai nagrinėjamas pasaulinėje mokslinėje literatūroje (taip pat ir elektroninių rinkimų saugumo užtikrinimo kontekste), vis dar nėra sukurtas kibernetinio saugumo valdymo modelis, kuris savyje sujungtų visapusišką požiūrį į kibernetinio saugumo grėsmes bei jų valdymo aspektus ir tokiu būdu suteiktų galimybę konstruoti maksimaliai saugias elektroninių rinkimų sistemas ir sėkmingai įgyvendinti elektroninius rinkimus.

Mokslinė problema: kokios yra kibernetinio saugumo sritys ir kaip turi būti organizuojamas kibernetinio saugumo valdymas, siekiant saugių ir patikimų elektroninių rinkimų įgyvendinimo?

Tyrimo objektas – elektroninių rinkimų įgyvendinimas kibernetinio saugumo valdymo kontekste.

Tyrimo tikslas – išanalizavus teorinio kibernetinio saugumo valdymo problematiką, sukurti kibernetinio saugumo valdymo modelį, kuris gali būti naudojamas įgyvendinant elektroninių rinkimų sistemas.

Siekiant tikslo, disertacijoje sprendžiami tokie **uždaviniai:**

1. Išanalizuoti kibernetinio saugumo valdymo teorinius aspektus, siekiant nustatyti pagrindines kibernetinio saugumo incidentų atsiradimo priežastis ir ypatumus, kibernetinio saugumo valdymo problematiką bei galimą kibernetinio saugumo incidentų įtaką elektroninių rinkimų sistemų kibernetiniam saugumui.
2. Išanalizuoti pasaulyje įvykdytas praktines atakas prieš elektroninių rinkimų sistemas, siekiant nustatyti ir išryškinti labiausiai pažeidžiamus e-rinkimų sistemų elementus.
3. Atsižvelgiant į teorinių kibernetinio saugumo valdymo aspektų analizės metu išryškėjusią kibernetinio saugumo valdymo problematiką, sukurti konceptualų kibernetinio saugumo valdymo modelį, taikytiną elektroninių rinkimų sistemų konstravimo, diegimo, valdymo ir naudojimo procesų metu, bei atlikti sukurto modelio vertinimui skirtą empirinį tyrimą.
4. Atsižvelgiant į empirinio tyrimo rezultatus, patikslinti konceptualų kibernetinio saugumo valdymo modelį, atlikti modelio struktūros, taikymo galimybių bei ribotumų analizę, pateikiant rekomendacijas, kaip modelis gali būti panaudojamas, įgyvendinant elektroninius rinkimus Lietuvoje.

Mokslinio tyrimo metodai. Disertacinis tyrimas yra suplanuotas trimis etapais. Pirmajame tyrimo etape, tiriant problema teoriniame lygmenyje, bus atliekama mokslinės literatūros ir kitų šaltinių analizė, palyginimas ir apibendrinimas, nagrinėjamos kibernetinių incidentų atsiradimo priežastis bei problematika. Antrajame disertacinio tyrimo etape bus formuojamas pradinis teorinis kibernetinio saugumo valdymo modelis elektroniniams rinkimams įgyvendinti, bei bus atliktas empirinis tyrimas (ekspertinis interviu). Siekiant išnagrinėti disertacinio darbo mokslinę problemą ekspertinio interviu metu bus apklausi ekspertai tiesiogiai dirbantys su kibernetinio saugumo valdymu ir įgyvendinimu, kibernetinio saugumo strategijos ir politikos formavimu bei technologiniu kibernetinio saugumo užtikrinimu. Trečiajame tyrimo etape, atsižvelgiant į empirinio tyrimo rezultatus, bus atliekamas teorinio kibernetinio saugumo valdymo modelio koregavimas, bei pateikiamą patikslinto kibernetinio saugumo valdymo modelio elektroniniams rinkimams įgyvendinti struktūros analizė. Tyrimo pabaigoje bus panaudojamas apibendrinimo metodas formuluojant teorinio ir empirinio tyrimų išvadas, taip pat pateikiamos rekomendacijos elektroninių rinkimų įgyvendinimui.

Disertacijos ginamieji teiginiai:

1. Kibernetinio saugumo valdymas dažniausiai suprantamas kaip technologinių priemonių taikymas organizacijos veiklos procesuose, tačiau tokia kibernetinio saugumo valdymo samprata yra labai ribojanti ir neapimanti visos organizacijos

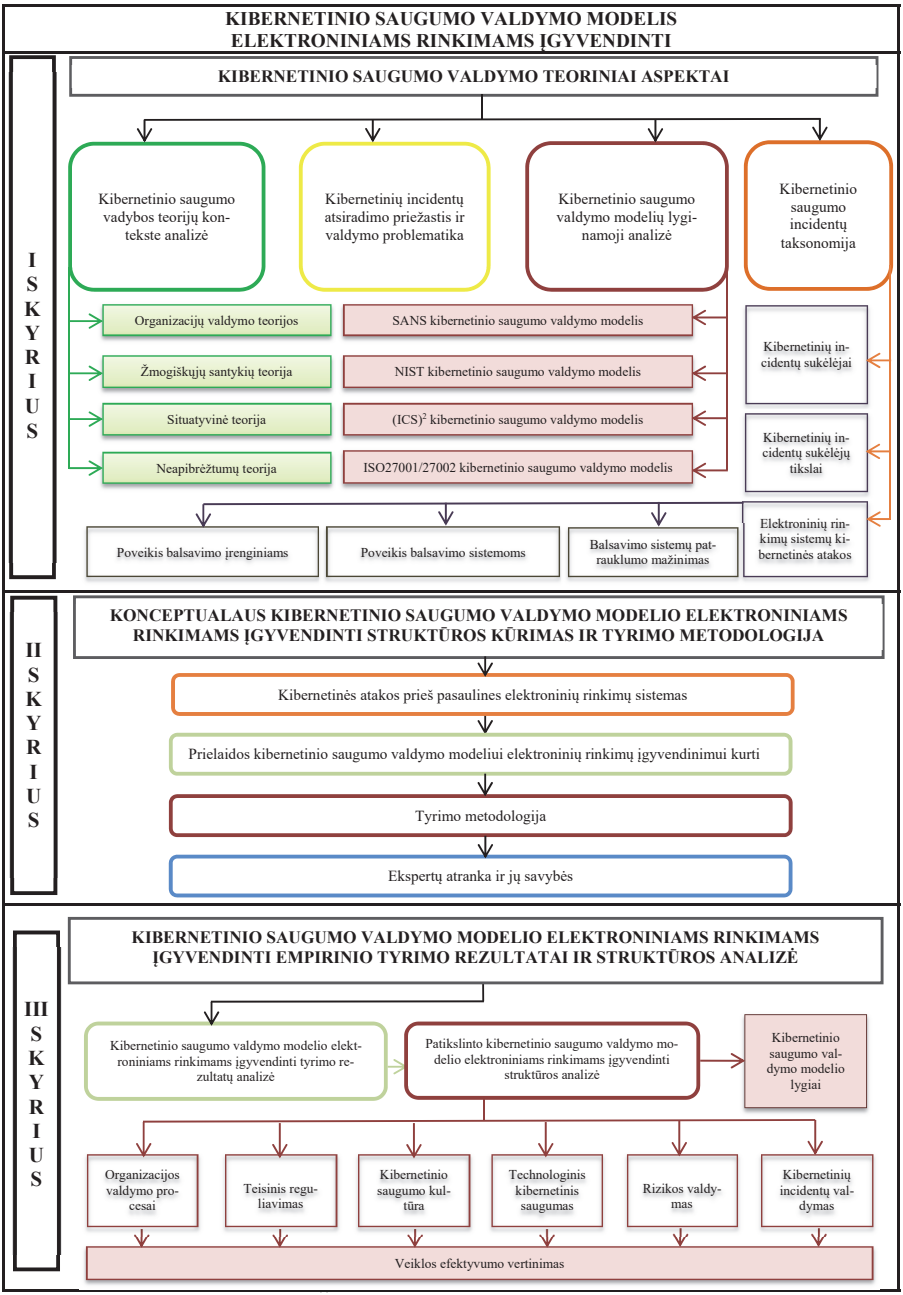
veiklos sričių: vadovavimo, teisinio reguliavimo, technologijų, rizikų ir incidentų valdymo, organizacijos saugumo kultūros.
2. Kibernetinio saugumo valdymo modelis, kuriame yra integruotos technologinės, teisinės, organizacinės bei fizinės saugos priemonės, gali būti naudojamas, kuriant saugią ir patikimą elektroninių rinkimų sistemą.
3. Sukurto kibernetinio saugumo valdymo modelio panaudojimas elektroninių rinkimų sistemų kūrimo ir diegimo procese suteikia galimybę valstybės piliečiams labiau pasitikėti sistemomis, kurios naudojamos elektroniniams rinkimams, bei gali paskatinti piliečius aktyviau dalyvauti valstybių politiniuose procesuose.

Darbo naujumas ir praktinis reikšmingumas. Pasaulyje kibernetinio saugumo reiškinys yra tiriamas įvairių mokslo šakų, dažniausiai – gamtos, technologijų ir socialinių sričių mokslininkų. Tačiau pažymėtina, kad mokslininkai nagrinėja kibernetinio saugumo valdymo problemą išskirtinai savo mokslo srities kontekste, nesigilindami į kitų mokslo šakų formuojamą problematiką. Taip sukuriama ydinga praktika, kai kibernetinis saugumas suprantamas ne kaip vientisas reiškinys, sujungiantis savyje visas mokslo sritis, bet kaip atskirų mokslo sričių tyrimo objektas. Atkreiptinas dėmesys, kad vien tik kompleksiškas požiūris į kibernetinio saugumo valdymą gali suteikti galimybę visapusiškai įvertinti kibernetinio saugumo spragas bei identifikuoti geriausius šių spragų pašalinimo būdus ir metodus. Šio disertacinio darbo naujumas ir reikšmingumas pasireiškia tuo, kad į kibernetinio saugumo valdymą žvelgiama per įvairių mokslo sričių prizmę, taip pat kad yra sukuriamas ir nagrinėjamas kibernetinio saugumo valdymo modelis, kurio įgyvendinimas gali užtikrinti elektroninių rinkimų sistemos sukūrimą Lietuvoje.

Atlikus mokslinės literatūros ir kitų šaltinių analizę disertacijos tema, buvo identifikuoti kibernetinio saugumo pažeidžiamumus sąlygojantys veiksniai, sukurta kibernetinio saugumo incidentų taksonomija elektroninių rinkimų sistemų kontekste. Teorinių tyrimų metu taip pat buvo analizuojami pasaulio mokslininkų tyrimai, glaudžiai susiję su kibernetinio saugumo pažeidžiamumais šiuo metu veikiančiose ar anksčiau veikusiose elektroninių rinkimų sistemose. Vadovaujantis teorinių tyrimų metu sukauptais duomenimis, buvo sukurtas pradinis kibernetinio saugumo valdymo modelis, kuris gali būti naudojamas elektroninių rinkimų sistemų kibernetiniam saugumui užtikrinti, bei atliktas šio modelio empirinis tyrimas, suteikęs tyrėjui galimybę patikslinti pradinį kibernetinio saugumo valdymo modelį ir pritaikyti jį elektroninių rinkimų sistemoms įgyvendinti.

Disertacinis darbas identifikuoja bendrus šiuolaikinio kibernetinio saugumo valdymo probleminius aspektus organizacijose, taip pat pasiūlo šių problemų sprendimo metodus bei aiškiai apibrėžia kibernetinio saugumo valdymo modelį, kuris gali būti panaudojamas, kuriant ir diegiant elektroninių rinkimų sistemas. Disertaciniame darbe pateikiamas kibernetinio saugumo valdymo modelis taikytinas, siekiant užtikrinti sklandų kibernetinio saugumo valdymo procesą, kuriant ir įgyvendinant elektroninių rinkimų sistemas Lietuvoje, taip pat vykdant jų eksploatavimą. Tikėtina, kad, naudojant sukurtą, techniškai neutralų, kibernetinio saugumo valdymo modelį, elektroninių rinkimų sistemų įgyvendinimas ir naudojimas Lietuvoje greitu laiku taps realybe.

Disertacinio darbo struktūra. Disertacinį darbą sudaro trys dalys (žr. 1 paveikslą). *Pirmoje dalyje* yra nagrinėjami kibernetinio saugumo valdymo teoriniai aspektai: kibernetinis saugumas nagrinėjamas organizacijų valdymo, žmogiškųjų santykių, situatyvinės ir aplinkos neapibrėžtumo teorijų kontekstuose; analizuojami kibernetinio saugumo incidentų atsiradimo priežastys ir ypatumai; aptariama kibernetinio saugumo valdymo problematika; aptariami ir palyginami kai kurie pasaulyje egzistuojantys kibernetinio saugumo valdymo modeliai ir jų panaudojimas organizacijos veiklos procesuose; aptariamas kibernetinio saugumo valdymas elektroninių rinkimų sistemų kūrimo ir diegimo kontekste; pateikiama kibernetinio saugumo taksonomija, aprašanti kibernetinio saugumo incidentų rūšis, incidentų sukėlėjus ir jų tikslus, kibernetinių nusikaltėlių taikomus kibernetinių atakų metodus; nagrinėjami elektroninių balsavimo sistemų pažeidžiamumai. *Antroje dalyje* pristatomas teorinių įžvalgų pagrindu sukurtas konceptualus kibernetinio saugumo valdymo modelis ir vykdyto empirinio tyrimo metodologija. *Trečioje dalyje* aprašomi kibernetinio saugumo valdymo modelio empirinio tyrimo rezultatai, pateikiama detali kibernetinio saugumo valdymo modelio struktūros analizė bei nagrinėjamas sukurto kibernetinio saugumo valdymo modelio pritaikomumas, įgyvendinant elektronines rinkimų sistemas Lietuvoje. *Darbo pabaigoje* yra pateikiamos išvados ir rekomendacijos.



Šaltinis: *parengta autoriaus*

1 paveikslas. *Disertacinio darbo struktūros loginė schema*

PIRMOSIOS DALIES APŽVALGA: KIBERNETINIO SAUGUMO VALDYMO TEORINIAI ASPEKTAI

Pirmojoje disertacijos dalyje yra aptariama kibernetinio saugumo valdymo svarba šiuolaikiniame, technologijomis grindžiamame, pasaulyje, kibernetinis saugumas yra nagrinėjamas kai kurių vadybos teorijų kontekste. Taip pat yra nagrinėjama kibernetinio saugumo reiškinio apibrėžimo kaita ir evoliucionavimas. Būtent apibrėžimų gausa, skirtingas jų traktavimas, skirtingų apibrėžimų lygiagretus evoliucionavimas lėmė, kad informacinių technologijų saugumo apibrėžimas ir jo suvokimas pasauliniame kontekste suponuoja daugybės skirtingų kibernetinio saugumo sąvokų visumos atsiradimą ir traktavimą. Kompiuterių saugumo reiškinio virsmas į duomenų saugumą, vėliau – į informacijos saugumą ir kibernetinį saugumą sudarė prielaidas kibernetinio saugumo reiškinį tapatinti vien tik su technologinėmis priemonėmis, kurios yra naudojamos informacinių išteklių apsaugai nuo kibernetinių incidentų. Tačiau pastebėtina, kad dabartiniu laikotarpiu kibernetinio saugumo reiškinys turi būti suvokiamas daug plačiau nei tik technologinių priemonių taikymas, siekiant išvengti kibernetinių incidentų ir juos stabdyti.

Pirmojoje disertacijos dalyje taip pat yra nagrinėjamos ir pateikiamos kibernetinių incidentų atsiradimą sąlygojančios priežastys, analizuojama kibernetinio saugumo valdymo problematika, įvardinamos viešojo ir privataus sektorių organizacijų klaidingos nuomonės ir daromos sisteminės klaidos, kurios neigiamai atsiliepia organizacijos kibernetinio saugumo užtikrinimo proceso formavimui. Taip pat yra atliekama kai kurių pasaulyje naudojamų kibernetinio saugumo valdymo modelių lyginamoji analizė, pateikiami nagrinėtų modelių privalumai ir trūkumai, nagrinėjamas jų tinkamumas kibernetinio saugumo valdymo užtikrinimo kontekste.

Nagrinėjant kibernetinio saugumo teorinius aspektus, disertacijos pirmoje dalyje didelis dėmesys yra skiriamas elektroniniams rinkimams ir elektroninių rinkimų sistemoms. Disertacijoje yra pateikiamas naujas požiūris į elektroninių rinkimų sistemoms kylančias grėsmes – pateikiama kibernetinio saugumo incidentų taksonomija, kurioje atkreipiamas dėmesys ne tik į tradicines (labiausiai paplitusias) kibernetines atakas ir incidentus, bet įvardinamos galimos ateities kibernetinių atakų tendencijos, identifikuojant naujus kibernetinių incidentų sukėlėjų tikslus, atakų taikinius, būdus bei metodus. Taip pat šioje dalyje yra analizuojamos teorinės bei praktinės kibernetinės atakos prieš veikiančias ar praeityje veikusias kai kurių pasaulio šalių elektroninių rinkimų sistemas, kurios buvo įvykdytos, siekiant surasti balsavimo sistemų spragas arba kompromituoti realiai veikiančias informacines rinkimų sistemas arba jose panaudotus technologinius įrenginius (balsavimo terminalus).

ANTROSIOS DALIES APŽVALGA: KONCEPTUALAUS KIBERNETINIO SAUGUMO VALDYMO MODELIO ELEKTRONINIAMS RINKIMAMS ĮGYVENDINTI STRUKTŪROS KŪRIMAS IR TYRIMO METODOLOGIJA

Antroji disertacinio darbo dalis skirta kibernetinio saugumo valdymo modelio empirinio tyrimo metodikai pagrįsti, tyrimo metodų ir procedūrų sekai aprašyti. Pirmajame ir antrajame poskyriuose aprašomos elektroninių rinkimų sistemų kibernetinės atakos, kibernetinio saugumo valdymo modelio kūrimo prielaidos bei principai, taip pat pateikiama preliminari kibernetinio saugumo valdymo modelio struktūra. Trečiame ir ketvirtame poskyriuose pateikiama siūlomo kibernetinio saugumo valdymo modelio tyrimo metodika, panaudota empirinio tyrimo organizavimo metu, paaiškinami ekspertų atrankos kriterijai.

Empiriniam tyrimui atlikti buvo pasirinktas pusiau struktūruoto interviu metodas, kurio metu buvo apklausti 9 kibernetinio saugumo ekspertai. Akcentuotina, kad technologinio kibernetinio saugumo užtikrinimas negali būti traktuojamas kaip pakankama priemonė, užtikrinanti kibernetinį saugumą organizacijoje. Būtent dėl šios priežasties siūlomas kibernetinio saugumo valdymo modelis yra technologiškai neutralus. Taip pat, siekiant išvengti vien tik technologijomis grindžiamo požiūrio į kibernetinį saugumą, tyrimo imties sudarymo metu buvo pasirenkami ekspertai, kurių žinios ir patirtis kibernetinio saugumo srityje yra siejama ne tik su technologinių apsaugos priemonių panaudojimu kibernetiniam saugumui užtikrinti, bet ir su kibernetinio saugumo politikos formavimu, teisiniu reglamentavimu, strateginio kibernetinio saugumo planavimu ir vystymu. Toks ekspertų parinkimo metodas užtikrina, kad pasirinkti ekspertai bus susipažinę ne tik su technologinės kibernetinio saugumo problemos sprendimo būdais, bet suvoks ir turės patirties kitose kibernetinio saugumo užtikrinimo srityse. Šios anksčiau išvardytos ekspertų kompetencijos ir praktinio darbo kibernetinio saugumo srityje patirtis leidžia teigti, kad atlikto empirinio tyrimo rezultatai bus patikimi ir išsamūs.

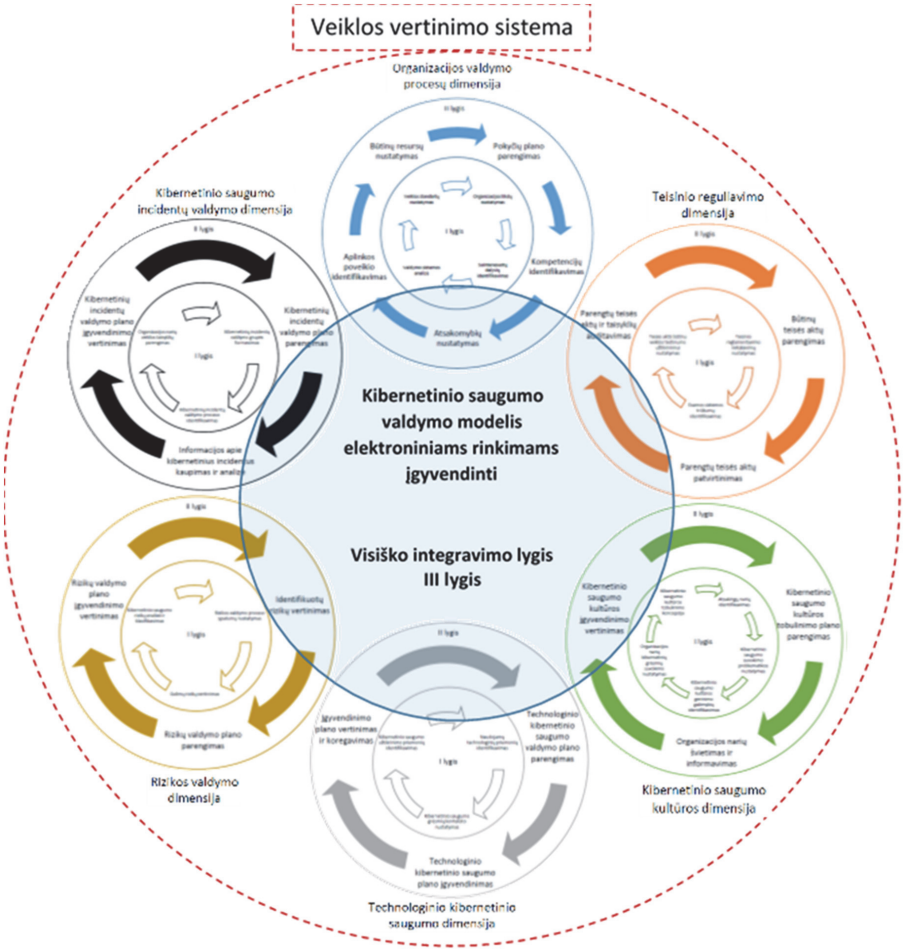
TREČIOSIOS DALIES APŽVALGA: KIBERNETINIO SAUGUMO VALDYMO MODELIO ELEKTRONINIAMS RINKIMAMS ĮGYVENDINTI EMPIRINIO TYRIMO REZULTATAI IR STRUKTŪROS ANALIZĖ

Trečioji disertacijos dalis yra skirta siūlomo kibernetinio saugumo valdymo modelio empirinio tyrimo rezultatams aptarti ir apibendrinti. Atlikus kibernetinio saugumo valdymo modelio empirinį tyrimą, tyrimo metu gauti rezultatai ir ekspertų siūlymai buvo panaudoti, patikslinant koncepcinį kibernetinio saugumo valdymo modelį, jį papildant papildomais elementais, kurie yra būtini, siekiant užtikrinti visapusišką kibernetinio saugumo valdymo procesą elektroninių rinkimų sistemų įgyvendinimo metu.

Šioje disertacijos dalyje taip pat yra atliekama patikslinto kibernetinio saugumo valdymo modelio struktūros analizė, pateikiamos kibernetinio saugumo valdymo modelio dimensijų priemonių įgyvendinimo rekomendacijos, kurių turi būti laikomasi, siekiant sukurti bei įgyvendinti veiksmingą ir saugią elektroninių rinkimų sistemą Lietuvoje.

Apibendrinus kibernetinio saugumo valdymo modelio empirinio tyrimo rezultatus, konceptualus pradinis kibernetinio saugumo valdymo modelis yra papildytas veiksmingumą didinančiais elementais (žr. 2 paveikslą).

Pažymėtina, kad *iš visų šešių kibernetinio saugumo valdymo modelyje nagrinėjamų dimensijų neįmanoma išskirti vienos pačios svarbiausios, kadangi tik visų šešių kibernetinio saugumo valdymo dimensijų priemonių įdiegimas organizacijoje bei šių dimensijų sujungimas į vieną bendrą organizacijos kibernetinio saugumo valdymo sistemą gali parodyti aiškius kibernetinio saugumo pokyčio rezultatus*. Kiekviena modelio dimensija gali būti vystoma atskirai, numatant skirtingus pirmojo ir antrojo lygio priemonių įgyvendinimo laikus, atsižvelgiant į organizacijos veiklos ypatumus, valdomus išteklius, turimus resursus bei finansines galimybes. Tačiau būtina pažymėti, kad visų *kibernetinio saugumo valdymo modelio dimensijų trečiasis lygmuo yra siejamas su pavienių ir tarpusavyje nepriklausomų organizacijos kibernetinio saugumo valdymo procesų (dimensijų) virsmu į integruotą kibernetinio saugumo valdymo sistemą, kurios komponentai yra vienareikšmiškai susieti bei veikia vienas kitą*.



Šaltinis: *Sudaryta autoriaus pagal Limba, Agafonov ir kt., 2017*

2 paveikslas. *Kibernetinio saugumo valdymo modelis elektroniniams rinkimams įgyvendinti*

IŠVADOS IR REKOMENDACIJOS

1. Atlikus mokslinių šaltinių analizę, siekiant atskleisti kibernetinio saugumo valdymo teorinius aspektus bei įvardyti pagrindines kibernetinio saugumo incidentų atsiradimo priežastis ir ypatumus, kibernetinio saugumo valdymo problematiką bei galimą kibernetinio saugumo incidentų įtaką ir poveikį elektroninių rinkimų sistemų kibernetiniam saugumui, nustatyta kad:
   1.1. Kibernetinio saugumo apibrėžimų įvairovė suponuoja šio reiškinio suvokimo problematiką ne tik visuomenės sluoksniuose, kasdien tiesiogiai nesusiduriančiose su šiuo reiškiniu, bet ir tarp asmenų, kurie tiesiogiai dirba su kibernetinio saugumo užtikrinimo iššūkiais. Šiuolaikinis kibernetinis saugumas turi būti traktuojamas ne tik kaip technologinė disciplina, bet kaip vientisas sudėtingas reiškinys, kuriame yra nagrinėjami techniniai, teisiniai, personalo, organizacijos valdymo ir kitų mokslų aspektai;
   1.2. Informacinių ir ryšio technologijų skvarbos ir jų įtakos įvairioms visuomenės gyvenimo sritims didėjimas sudaro sąlygas kibernetinio saugumo grėsmių augimui ir sėkmingų kibernetinių atakų skaičiaus padidėjimui;
   1.3. Organizacijų pasitikėjimas esama valdomos infrastruktūros apsauga, informacinių sistemų aptarnaujančio personalo žiniomis, naudojama technologine įranga ir jos atliekamomis funkcijomis bei supančios aplinkos suvokimo problematika sukelia galimybes rengti sėkmingas kibernetines atakas prieš organizacijas ir sistemas;
   1.4. Šiuolaikiniame technologijomis grindžiamame pasaulyje keičiasi ne tik kibernetinio saugumo incidentų ir grėsmių rūšys, bet tobulėja ir kibernetinių incidentų sukėlėjų naudojamos atakų vykdymo priemonės. Atsiranda naujos atakų rūšys, kurių tikslas yra tiesiogiai nesusijęs su technologinių priemonių panaudojimu, siekiant diskredituoti informacines sistemas ar jų teikiamas paslaugas;
   1.5. Nors technologiniai kibernetinio saugumo pažeidžiamumai šiuolaikiniame pasaulyje ir yra laikomi viena iš svarbiausių saugumo pažeidžiamumų rūšimi, dabartiniu laikotarpiu vis dažniau žmogiškasis faktorius yra įvardijamas kaip priežastis, dėl kurios dažniausiai yra sėkmingai įgyvendinamos kibernetinės atakos. Siekiant apsaugoti informacinius išteklius nuo žmogiškojo faktoriaus įtakos, yra būtinas ne tik technologinių priemonių panaudojimas, bei šių priemonių automatizavimas, bet ir veiksmai, kuriais bus minimizuojama žmogiškojo faktoriaus įtaka kibernetiniam saugumui;
   1.6. Disertacinio darbo pirmojoje teorinėje dalyje nagrinėti pasaulyje naudojami organizacijų kibernetinio saugumo valdymo modeliai labiausiai yra orientuoti į technologinio kibernetinio saugumo užtikrinimą organizacijoje, tačiau modeliuose visiškai neaptariami arba menkai aptariami organizacijos, žmogiškųjų išteklių, rizikos ir incidentų valdymo aspektai;
   1.7. Atlikus kibernetinio saugumo incidentų, atakų ir galimų pažeidžiamumų analizę elektroninių rinkimų sistemų kontekste, disertacijoje yra pristatoma

elektroninių rinkimų sistemų kibernetinių incidentų taksonomija, kurioje yra išsamiai nagrinėjami ne tik tradiciniai kibernetinių atakų būdai, bei jos vykdantys asmenys, bet ir klasifikuojami kibernetinių nusikaltėlių tikslai, atakų taikiniai bei jų vykdymo būdai;

1.8. Valdymo sistemos sukūrimas ir pritaikymas elektroninių balsavimo sistemų konstravimo procese gali sudaryti galimybes eliminuoti daugumą nustatytų ir disertaciniame darbe aptartų pažeidžiamumų.

2. Teorinių įžvalgų pagrindu kuriant konceptualų kibernetinio saugumo valdymo modelį, kuris gali būti taikomas elektroninių rinkimų sistemų konstravimo, diegimo, valdymo ir naudojimo procesų metu, nustatyta, kad:
   2.1. Siekiant tinkamo kibernetinio saugumo valdymo organizacijoje, būtina nagrinėti šešias saugumo dimensijas: organizacijos valdymo procesų, teisinio reguliavimo, kibernetinio saugumo kultūros, technologinio saugumo, rizikos ir incidentų valdymo;
   2.2. Kibernetinio saugumo grėsmių valdymas, pasinaudojant šių dimensijų įgyvendinimo priemonėmis, gali padėti organizacijai sėkmingai kontroliuoti galimas rizikas ir pažeidžiamumus bei sumažinti sėkmingų kibernetinių išpuolių poveikį valdomiems ištekliams;
   2.3. Didžiausias iššūkis yra susijęs su technologinių žinių ir valdymo procesų sujungimu, nes dažniausiai techninis personalas ir valdymo specialistai skirtingai traktuoja kibernetinio saugumo valdymo aspektus;
   2.4. Organizacijos pokyčiai kibernetinio saugumo kontekste prasideda tuomet, kai saugumas organizacijoje pradedamas traktuoti ne tik kaip technologinė disciplina, bet kaip realus valdymo sistemos kaitos iššūkis;
   2.5. Kibernetinio saugumo valdymo modelis taip pat suteikia galimybę organizacijos lyderiams aktyviai dalyvauti, priimant sprendimus ir kuriant kibernetinio saugumo politiką, bei įgalina organizaciją tinkamai vertinti saugumo rizikas ir jų mažinimo priemones;
   2.6. Kibernetinio saugumo valdymo modelio įdiegimas taip pat gerina organizacijos reputaciją išorinėje aplinkoje, nes organizacija, kuri rūpinasi savo kibernetiniu saugumu, yra patrauklesnė vartotojams ar verslo partneriams;
   2.7. Disertaciniame darbe siūlomo valdymo modelio idėja ir aktualumas yra siejami su naujo požiūrio į kibernetinį saugumą formavimu, kuomet jis yra taikomas visos organizacijos veiklos procesams, o kiekvienas organizacijos narys privalo dalyvauti kibernetinio saugumo gerinime;
   2.8. Organizacijos izoliavimas nuo išorinio pasaulio ir jame egzistuojančių kibernetinių grėsmių yra neįmanomas, o diegiamas kibernetinio saugumo valdymo modelis turi nagrinėti ne tik organizacijos vidaus aplinką, bet ir jos sąveiką su išorine aplinka.

3. Atlikus empirinio tyrimo metu siūlomo kibernetinio saugumo valdymo modelio vertinimą bei apibendrinus pusiau struktūrizuoto ekspertų interviu metu gautus rezultatus, nustatyta, kad:

3.1. Siūlomo kibernetinio saugumo valdymo modelio komponentai: organizacijos valdymo procesų, teisinio reguliavimo, kibernetinio saugumo kultūros, technologinio saugumo, rizikos ir incidentų valdymo dimensijos, turi būti naudojami kuriant kibernetinio saugumo valdymą;
3.2. Siūlomas modelis turintis veiklos efektyvumo vertinimo sistemą, suteikia organizacijai galimybę stebėti kibernetinio saugumo valdymo įgyvendinimo pokyčius konkrečiose dimensijose, taip pat nustatyti organizacijos kibernetinio saugumo valdymo evoliucionavimo procesą;
3.3. Siūlomo kibernetinio saugumo valdymo modelio įgyvendinimas tūri būti atliekamas laipsniškai (pakopomis, lygiais);
3.4. Organizacijos valdymo procesų dimensijos įtaka saugumo kūrimui organizacijoje gali būti apibūdinama kaip lemiamas kibernetinio saugumo valdymo įgyvendinimo procesas. Organizacijos vykdomos veiklos koregavimas ir pritaikymas kibernetinio saugumo procesams užtikrinti keičia organizacijos veiklos modelį bei atveria galimybes pažeidžiamumams mažinti;
3.5. Teisinis reguliavimas yra neatsiejamas nuo kibernetinio saugumo valdymo. Šios dimensijos ribose yra užtikrinamas organizacijos teisinio reglamentavimo sukūrimas, suteikiantis organizacijai galimybę administracinėmis priemonėmis didinti vidinės organizacijos aplinkos atsparumą kibernetinėms grėsmėms;
3.6. Įgyvendindama teisinio reguliavimo dimensiją, organizacija taip pat turi galimybę daryti įtaką ne tik vidinei, bet ir išorinei aplinkai, dalyvaujant kibernetinio saugumo teisinės bazės rengimo procese;
3.7. Siekiant sumažinti organizacijos pažeidžiamumą bei išvengti kibernetinių incidentų, yra privalomas visų, be išimties, darbuotojų mokymas ir švietimas, nepaisant darbuotojo užimamų pareigų. Toks kompleksinis požiūris suteikia galimybes eliminuoti galimas grėsmes (atakas), neatsižvelgiant į tai, į kokią personalo grupę jos yra orientuotos;
3.8. Bendradarbiaujant su partneriais, paslaugų tiekėjais, kitomis organizacijomis, būtina vertinti galimų partnerių kibernetinio saugumo valdymą, tokiu būdu sudarant galimybę išvengti savo valdomos infrastruktūros kompromitavimo bei galimų nuostolių;
3.9. Technologinis kibernetinis saugumas turi būti siejamas ne su konkrečių technologinių sprendimų parinkimu organizacijos saugumui užtikrinti, o vykdomas kaip technologiškai neutralus įrangos ir kibernetinio saugumo sprendimų valdymo procesas, numatantis būtinus organizacijos veiksmus, siekiant užtikrinti vykdomos veiklos tęstinumą, įrangos gyvavimo ciklo palaikymą, išteklių planavimą ir kt.;
3.10. Tik tinkamas rizikos įvertinimas, klasifikavimas bei jų mažinimo priemonių identifikavimas suteikia organizacijai galimybę nusimatyti galimų pažeidžiamumų vengimo ar mažinimo strategiją, subalansuojant ir minimizuojant šiam procesui skiriamus finansinius išteklius;

3.11. Kibernetinių incidentų valdymas organizacijoje turi būti suprantamas ne kaip reagavimas į vykstančią kibernetinę ataką ar jos padarinių šalinimas, bet kaip nenutrūkstamas procesas, kurio metu yra vertinama ne tik vidinė organizacijos valdoma infrastruktūra, bet ir išorės aplinka: kibernetinių incidentų plėtros tendencijos, atakų atlikimo metodai ir būdai, technologinių atakų alternatyvos ir kt.;

3.12. Tinkamas kibernetinio saugumo kultūros kūrimas ne tik organizacijoje, bet visos valstybės mastu, gali tapti visuotinio kibernetinio saugumo pagerėjimo priežastimi, bet šie gebėjimai privalo būti ugdomi visuose lygmenyse, pradedant nuo švietimo sistemos pradinio ugdymo programų;

3.13. Sukurti saugią elektroninių rinkimų sistemą yra įmanoma, tik įtikinus šios sistemos naudotojus (piliečius), kad jų balsai, atiduoti technologijomis grindžiama rinkimų sistema, nebus suklastoti, o rinkimų rezultatais nebus manipuliuojama;

3.14. Būtina tinkamai informuoti visuomenę, siekiant tinkamo visuomenės nuomonės apie elektroninius rinkimus susiformavimo. Nuomonės formavimas viešoje erdvėje, į kurį yra įtrauktos pilietinės visuomenės organizacijos, valstybės ir savivaldybių atstovai, medija, kibernetinio saugumo ekspertai ir kitos suinteresuotosios asmenų grupės, gali paskatinti visuomenę maksimaliai pasitikėti elektroniniais balsavimais, ir paspartinti šios sistemos įdiegimą, kas yra ypač aktualu dabartiniais pandemijos laikais.

Mokslinės publikacijos disertacijos tema

1. Limba T., Plėta T., Agafonov K., Damkus M., 2017. Cyber security management model for critical infrastructure, Entrepreneurship and Sustainability Issues 4(4): p. 559-573, <http://dx.doi.org/10.9770/jesi.2017.4.4(12)>.
2. Limba, T.; Agafonov, K.; Paukštė, L.; Damkus, M.; Plėta, T. 2017. Peculiarities of cyber security management in the process of internet voting implementation, Entrepreneurship and Sustainability Issues 5(2): 368-402, <https://doi.org/10.9770/jesi.2017.5.2(15)>.
3. Plėta, T.; Tvaronavičienė, M.; Casa, S. D.; Agafonov, K., 2020. Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases, Insights into Regional Development 2(3): p. 703-715, <https://doi.org/10.9770/IRD.2020.2.3(7)>.

Pranešimai mokslinėse konferencijose

4. Agafonov K., Limba T., Damkus M. Žodinis pranešimas. *Cyber Security: From Technology to Management*. Social Innovations: Theoretical and Practical Insights, 16th International Interdisciplinary Conference on Social Innovations, September 2016, Vilnius, Lithuania.
5. Agafonov K., Limba T., Plėta T., Damkus M. Žodinis pranešimas. *Kibernetinio saugumo ypatumai organizuojant balsavimą internetu*. Tarptautinė mokslinė konferencija „Komunikacijos ir informacijos mokslai tinklaveikos visuomenėje: patirtys ir įžvalgos IV“, 2018 m. birželio 14–15 d.

GYVENIMO APRAŠYMAS

Asmeninė informacija

Vardas, pavardė	Konstantin Agafonov
El. paštas	ka1979@gmail.com

Išsilavinimas

2015–2021	Vadybos mokslo krypties Mykolo Romerio universiteto doktorantas
2006–2008	Viešojo administravimo magistras, Mykolo Romerio universitetas
1997–2001	Informatikos bakalauras, Klaipėdos universitetas

Darbo patirtis

Nuo 2005	Krašto apsaugos sistema, karininkas
2008–2012	Mykolo Romerio universitetas, lektorius
2004–2005	Klaipėdos m. „Kuršių“ vidurinė mokykla, tinklo administratorius
2003–2004	UAB „Technolitika“, inžinierius-vadybininkas
2002–2003	AB „Laivitė“, informatikos inžinierius
2001–2002	UAB „Skaidula“, vadybininkas

MYKOLAS ROMERIS UNIVERSITY

Konstantin Agafonov

CYBERSECURITY MANAGEMENT MODEL FOR IMPLEMENTATION OF ELECTRONIC ELECTIONS

Summary of Doctoral Dissertation
Social Sciences, Management (S 003)

Vilnius, 2021

This doctoral dissertation has been prepared during the period of 2015–2021 at Mykolas Romeris University under the doctoral program right conferred to Vytautas Magnus University, Klaipėda University, Mykolas Romeris University and Šiauliai University by the order of the Minister of Education, Science and Sports of the Republic of Lithuania No. V-160 dated February 22, 2019.

Scientific Supervisor:
Prof. Dr. Tadas Limba (Mykolas Romeris University, Social Sciences, Management, S 003).

The doctoral dissertation will be defended at the Committee of Management of Vytautas Magnus University, Klaipėda University, Mykolas Romeris University and Vilnius University Šiauliai Academy:

Chairperson:
Prof. Dr. Rima Žitkienė (Mykolas Romeris University, Social Sciences, Management, S 003).

Members:
Prof. Dr. Vida Davidavičienė (Vilnius Gediminas Technical University, Social Sciences, Management, S 003);
Prof. Dr. Fernando Galindo (University of Zaragoza, Spain, Social Sciences, Law, S 001);
Prof. Dr. Rimantas Stašys (Klaipėda University, Social Sciences, Management, S 003);
Prof. Dr. Diana Šaparnienė (Vilnius University Šiauliai Academy, Social Sciences, Management, S 003).

The doctoral dissertation will be defended at the open meeting of the Scientific Council in the field of Management on October 7, 2021 at 11:00 at Mykolas Romeris University, I-414 Room. Address: Ateities st. 20, Vilnius, Lithuania.

The summary of the doctoral dissertation has been distributed on September 7, 2021.

The doctoral dissertation can be viewed at Martynas Mažvydas National Library of Lithuania (Gedimino ave. 51, Vilnius), libraries of Klaipėda University (K. Donelaičio ave. 3, Klaipėda), Mykolas Romeris University (Ateities str. 20, Vilnius), Vilnius University Šiauliai Academy (Vytauto st. 84, Šiauliai), Vytautas Magnus University (K. Donelaičio str. 52, Kaunas).

Konstantin Agafonov

CYBERSECURITY MANAGEMENT MODEL FOR IMPLEMENTATION OF ELECTRONIC ELECTIONS

SUMMARY

Relevance of the topic. Modern society, life and social relationships depends on cyberspace. Information technology professionals and researchers make great efforts to address cybersecurity issues. Information security standards have been developed and used since last decade of twentieth century, but they are more closely related to information security and technology management within the organization, whereas nowadays cybersecurity covers not only the management of information security threats and technological security, but also the monitoring of potential risks, incident response, threat assessments and prevention measures, staff training and legislation. Computer systems and technology solutions used to organize private sector activities are nowadays widely used in the public sector, while dialog between the state and its citizens is being phased into the digital space and results faster delivery of public services to citizens also reduce the workload on public administrations. The technological revolution causes that attempts to use modern information and telecommunications technology in the political process. States are trying to use technology to bring citizens closer to governance process, to activate direct participation in the various political processes taking place in the country. One of the most commonly used tools for political participation and involvement of the population in political processes is electronic voting.

The modern world has reached a very high level of technology development, but it is still not secure in terms of cybersecurity: growing number of cybersecurity incidents, sophisticated and difficult to detect intrusion technologies are widely used by cybercriminals (Simmons et al., 2014) and cybersecurity technology tools are not capable to detect and stop cyber attacks (Shabut et al., 2016). There are a lot of researches related to information security management in organizations: information security is examined not only in technical fields but also in management, economics and other sciences (Ashenden, 2008; Bakshi et al., 2009; Jastiuginas, 2011; Johnson, 2015), however, this researches are very fragmented and not sufficient to develop a cybersecurity management model that will explicitly and unambiguously define aspects of cybersecurity management during the development of state information systems and provision of electronic services to citizens. Although there is no common cybersecurity management model, but countries around the world understand the need to manage and carefully protect their information resources, and scientists have noted that security of critical infrastructure in a country is necessary and must be managed in an integrated manner (Limba ir kt., 2017; NATO StratCom COE, 2018; Haynes, 2019; Giniotienė 2019; Sofiou, 2019).

The phenomenon of cybersecurity has been under discussion since the 1990's. Noteworthy is that the meaning of this term has changed since its inception, and this change is associated with the advancement and change of technology. Cybersecurity (information security) phenomenon was started in the context of security of information processed by telecommunication and computer systems, later in the context of security of information transmitted in computer systems and finally in the context of ensuring the integrity, availability, authenticity, reliability and confidentiality of information.

Public sector, politicians, scientists and technology security experts agree that solving technological issues alone will not eliminate all the problems until a cybersecurity governance model for electronic elections is in place. In essence, the problem lies in the fact that cybersecurity must be treated not only as a technical discipline or attainable technical level (Lowrie, 2015), but as an organization management concept (Rainer et al., 2007). Concept that aggregates technical, legal (Štitilis et al., 2017), and most importantly, management strategies and achieving a certain maturity of the organization (Lackram, Padayachee, 2018; Patiño, Yoo, 2018).

The problem of cybersecurity management in the context of electronic elections is very relevant. In 2014 The United Nations has launched a global cybersecurity monitoring project which should observe the implementation level over the word. The main purpose of this doctoral thesis is to develop a cybersecurity management model that could be applied during the development of electronic voting systems. The implementation of electronic elections is one of the main ways of promoting citizen participation in the state political processes, and the major disadvantage of these systems is the lack of security. The cybersecurity management model, which will be developed and explored in the dissertation, will accelerate the implementation of secure electronic voting systems and recognition of electronic elections.

The level of exploration of the topic. Scientists, researchers, international organizations, cybersecurity technology and software experts and manufacturers analyze a lot of cybersecurity aspects.

There is still controversy in the scientific literature regarding the description of the cybersecurity phenomenon itself. The phenomenon of cybersecurity, its evolution and essence has been studied by Anderson, 2001; Ashenden, 2008; Jastiuginas, 2011; Agrawal, Campoe, Pierce, 2014; Alotaibi, Furnell, Clarke, 2016; Dykstra, 2017; Limba, Plėta, Agafonov, Damkus, 2017; Grincevičius, 2018 and other researchers.

Researchers Landwehr, Bull, McDermott, Choi, 1994; Howard, Longstaff, 1998; Weaver, Paxson, Staniford, Cullingham, 2003; Hansman, Hunt, 2003; Kjaerland, 2006; Gruschka, Jensen, 2010; Štitilis, 2011; Limba, Agafonov, 2012; Simmons, Shiva, Bedi, Dasgupta, 2014; Shabut, Lwin, Hossain, 2016 and other scientists describe cybersecurity incident and attack classification systems, identify possible ways and methods of conducting them.

Researchers also examine cybersecurity in legal terms: Štitilis, 2013; Appazov, 2014; Lowrie, 2015; Deighton, 2015; Štitilis, Klišauskas, 2015; Kosseff, 2018, aspects of Risk Management: Kroger, 2008; Ackermann, 2012; Agrawal, 2014; Chen, Pedrycz, Ma, Wang, 2014; Deighton, 2015; Proença, Estevens, Vieira, Borbinha, 2017; Vega, Arroyo,

Yoo, 2017; Walker, 2018; Grincevičius, 2018; Patiño, Solís, Yoo, Arroyo, 2018, aspects of Technology Security: Cayirci, Ghergherehchi, 2011; Solms, Niekerk, 2013; Donaldson, Siegel, Williams, Aslam, 2015; Alotaibi, Furnell, Clarke, 2016; Campbell, 2017; Collier, 2018, aspects of Incident Management: Deighton, 2015; Beissel, 2016; Craig, Valeriano, 2016; Limba, Agafonov, 2012; Process Management and Control Aspects: Rainer, Marshall, Knapp, Montgomery, 2007; Solms, 2009; Deighton, 2015; Latham & Watkins, 2016; Limba, Agafonov, Paukštė, Damkus, Plėta, 2017; Moschovitis, 2018; Patiño, Yoo, 2018.

Causes of cyber incidents are analyzed by Andersen, 2001; Barnes, Johnson, Nickelson, 2004; Masero, 2010; Wei, 2010; Cayirci, Ghergherehchi, 2011; Singer, Friedman, 2014; Craig, Valeriano, 2016; Voltz, 2016; Limba, Plėta, Agafonov, Damkus, 2017; Govindarasu, Han, 2017 and other researchers, also by various public and private sector organizations: ISO/IEC, 2013; US CERT, 2018; $(ISC)^2$, 2015; SANS, 2018, and others that over the past two decades have developed standards which could be used to ensure cybersecurity management in organizations.

Operation principles, cyber threats, theoretical and real vulnerabilities and attack methods of electronic voting systems were identified by researchers Jefferson, Rubin, Simons, Wagner, 2004; Kohno, Stubblefield, Rubin, Wallach, 2004; Filho, 2005; Feldman, Halderman, Felten, 2006; Hursti, 2006; Gonggrijp, Hengeveld, 2007; Simmons, 2011; Limba, Agafonov, 2012; Chowdhury, 2013; Aranha, Karam, Miranda, Scarel, 2014; Brightwell, Cucurull, Galindo, Guasch, 2015; Karda, Kiraz, Bingöl, Birinci, 2016; Goldsmith, 2017; Halderman, 2017; Limba, Agafonov, Paukštė, Damkus, Plėta, 2017; Augoye, Tomlinson, 2018 and others. Those researchers focused on identifying the causes of cyber incidents, in order to identify the critical factors affecting the use of electronic electoral systems in democratic processes.

Notably that in the global scientific literature cybersecurity is covered in many aspects (including in the context of electronic voting), but there is still no common cybersecurity management model that combines a comprehensive approach to cybersecurity threats and their management. Only this model will enable the ability to ensure development of secure e-voting systems and the successful implementation of electronic elections.

The scientific issue: what are the priority areas for cyber security management and how should cyber security management be organized to implement secure and reliable electronic elections?

The object of the research – implementation of electronic elections in the context of cyber security management.

The aim of the research – develop a cybersecurity management model for the implementation of electronic elections by analyzing theoretical issues of cybersecurity management. In order to achieve this goal, the dissertation addresses the following tasks:

1. To analyze the theoretical aspects of cybersecurity management in order to determine the root causes and features of cybersecurity incidents, the problems of cybersecurity management and the possible impact of cybersecurity incidents on the security of e-voting systems.

2. To analyze the practical attacks carried out in the world against electronic voting systems in order to identify and highlight the most vulnerable elements of e-voting systems.
3. To develop a conceptual cybersecurity management model applicable during the process of designing, implementing, managing and operating electronic election systems, and to carry out empirical research of the model, taking into account the problems of cybersecurity management revealed during the analysis of theoretical aspects of cybersecurity management.
4. Taking into account the results obtained during the empirical research, evaluate the cybersecurity management model, analyze its application possibilities and limitations, to provide recommendations how the model can be used in the implementation of e-voting in Lithuania.

Research methods. The research is planned in three stages. In the first phase of the research, the problem will be analyzed at the theoretical level. Also the causes and problems of the cyber incidents will be analyzed. In the second phase of the research the initial theoretical cybersecurity management model for the implementation of electronic elections will be identified, and an empirical study (expert interview) will be conducted. In order to examine the scientific issue expert interview will be conducted with experts directly involved in cybersecurity management, cybersecurity strategy and policy development and technological cybersecurity assurance. In the third stage of the research, based on the results of the empirical research, the theoretical cybersecurity management model will be adjusted and the structure analysis of the revised cybersecurity management model for electronic voting will be presented. At the end of the research, the generalization method will be used to formulate theoretical and empirical research findings, as well as recommendations for the implementation of electronic elections.

Defending statements:

1. Cybersecurity management is commonly understood as the application of technological tools in an organization operating processes, but this concept of cybersecurity management is very restrictive and does not cover the entire scope of an organization's activities: leadership, legislation, governance, organizational culture, etc.
2. The cybersecurity management model, which incorporates technological, legal, organizational and physical security measures, can be used to develop a secure and robust electronic voting system.
3. The use of the promoted cybersecurity management model in the design and deployment of electronic voting systems enables citizens to have greater confidence of that systems and can encourage citizens to become more involved in national political processes.

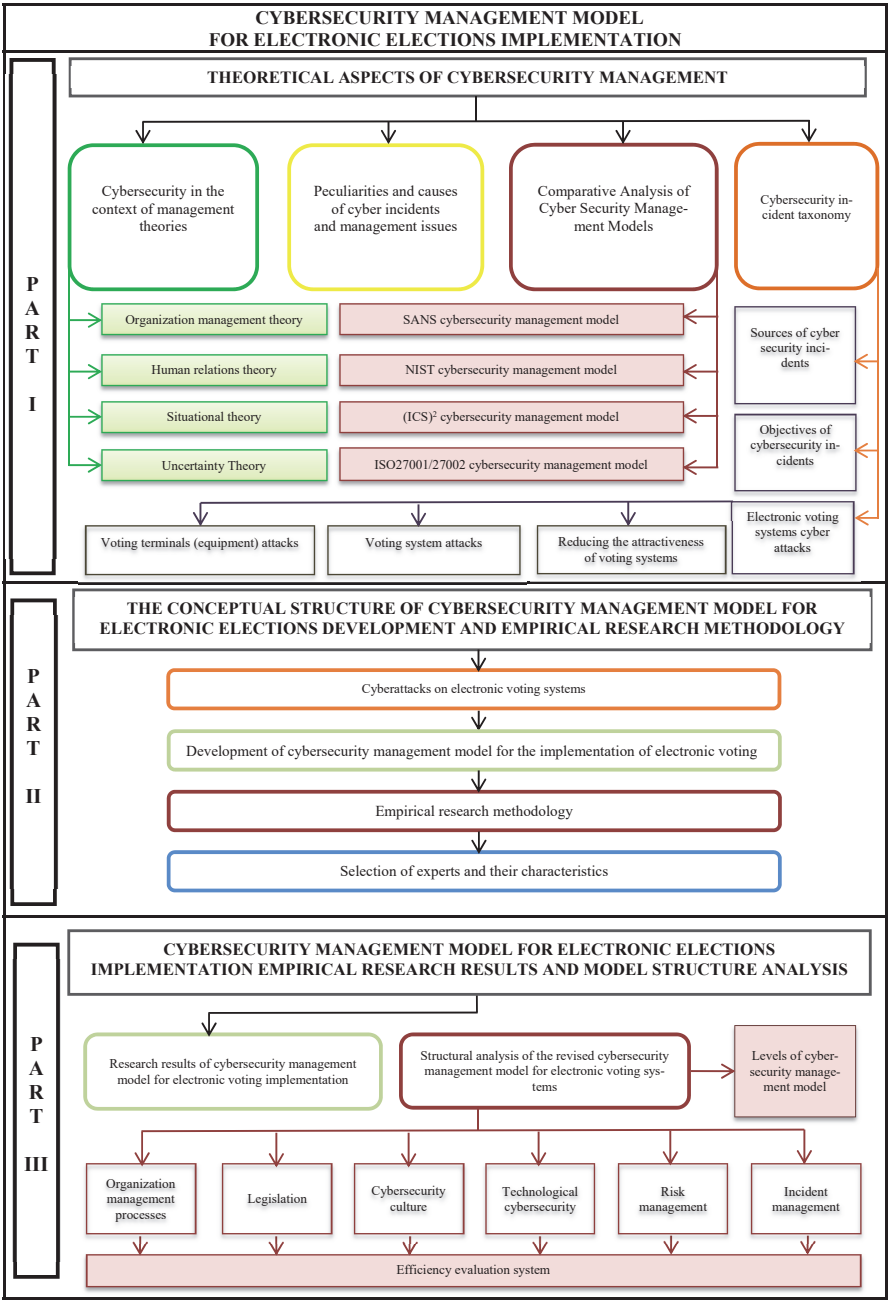
Novelty and practical significance of the research. The phenomenon of cybersecurity is being analyzed by researchers from various disciplines perspectives. However, it is noteworthy that researchers deal with the issue of cybersecurity management exclusively in the context of their field of science, without delving into the issues that are

emerging in other disciplines. This creates a flawed practice in which cybersecurity is not understood as a seamless interdisciplinary phenomenon that unites all scientific disciplines. It should be noted that a comprehensive approach to cybersecurity management can provide a comprehensive assessment of cybersecurity vulnerabilities and identify the best ways and methods to address these vulnerabilities. The novelty and significance of this doctoral thesis lies in the fact that cybersecurity management is viewed through the prism of interdisciplinary fields of science, as well as the presentation and analysis of a conceptual cybersecurity management model, which implementation will ensure the development of e-voting system in Lithuania.

After the analysis of scientific literature and other sources on the topic of the thesis, the factors determining the vulnerabilities of cybersecurity, the causes of the cyber incidents occurrence and the methods of cyber attacks were identified. Theoretical research has also analyzed the research of researches closely related to cybersecurity vulnerabilities in current or formerly operating electronic voting systems. Based on theoretical data, an initial cybersecurity management model, that can be used to secure voting systems, has been developed. An empirical study has been conducted to enable the researcher to refine the initial model and apply it to e-voting system implementation.

Thesis identifies common problematic aspects of modern cybersecurity management in organizations, proposes methods to address these problems, and clearly defines a cybersecurity model that can be used to develop and deploy electronic election. The cybersecurity management model presented in the dissertation is applicable to ensure a smooth cybersecurity management process in the development, implementation and operation of electronic voting systems in Lithuania. It is hoped that the implementation and use of electronic electoral systems in Lithuania will soon become a reality, using a developed, technically neutral, cybersecurity management model.

Structure of the research. Thesis consists of three parts (see Fig. 1). The first part deals with the theoretical aspects of cybersecurity management: cybersecurity is analyzed in the context of organizational management, situational, environmental uncertainty and human relations theories; the causes and peculiarities of cybersecurity incidents; cybersecurity management issues are discussed; discussing and comparing some of the world's existing cybersecurity management models and their use in organization working processes; discusses cybersecurity management in the context of developing and deploying electronic election systems; a cybersecurity taxonomy describing the types of cybersecurity incidents, their causes and their objectives, the cyber-attack methods used by cybercriminals; addressing vulnerabilities of electronic voting systems; theoretical and practical cyberattacks against electronic voting systems in the world, divided into two groups (online voting systems and electronic voting devices). The second part presents the conceptual model of cybersecurity management model based on theoretical insights and methodology of empirical research. The third part describes the results of the empirical research of the cybersecurity management model, provides a detailed analysis of the model's structure and examines the applicability of the developed cybersecurity management model in the implementation of electronic voting in Lithuania. Conclusions and recommendations are given at the end of the thesis.



Source: *prepared by the author*

Fig. 1. *The logical structure of the dissertation*

PART ONE OVERVIEW: THEORETICAL ASPECTS OF CYBERSECURITY MANAGEMENT

The first part of the doctoral thesis discusses the importance of cybersecurity management in the modern, technology-driven world. In this part cybersecurity is explored in the context of some management theories. Changes in the definition and evolution of the cybersecurity phenomenon are also explored. Abundance of cybersecurity definitions, their different treatment and the parallel evolution of different definitions that have led to the definition and understanding of information technology security in the global context, which implies the emergence and treatment of a whole host of different cybersecurity concepts. The transformation of the computer security phenomenon into data security and later into information security and cybersecurity, has made it possible to identify the cybersecurity phenomenon solely with the technological means used to protect information resources from cyber incidents. However, it is noteworthy that, in the current period, the cybersecurity phenomenon needs to be understood much wider than just the application of technological measures and tools to stop, prevent and eliminate cyber incidents.

The first part of the dissertation also examines and presents the reasons behind the emergence of cyber incidents, analyzes the problems of cybersecurity management, identifies misconceptions of public and private sector organizations and unclose systemic mistakes that negatively influence the formation of the cybersecurity process. There is also a comparative analysis of some cybersecurity management models used in the world, examined advantages and disadvantages of the models reveals their suitability in the context of ensuring cybersecurity .

In the first part of the dissertation special attention is paid to electronic elections and electronic voting systems. Thesis introduces a new approach to threats for the e-voting systems, providing a taxonomy of cybersecurity incidents that not only addresses traditional (most common) cyber attacks and incidents, but also identifies potential trends in future cyber attacks by identifying new aims, methods and actors. This section also analyzes the theoretical and practical cyber attacks on existing electronic voting systems, which have been conducted in order to address gaps in voting systems or to compromise voting systems or their technological equipment (voting terminals).

PART TWO OVERVIEW: THE CONCEPTUAL STRUCTURE OF CYBERSECURITY MANAGEMENT MODEL FOR ELECTRONIC ELECTIONS DEVELOPMENT AND EMPIRICAL RESEARCH METHODOLOGY

Second part of the doctoral thesis is devoted to the methodology of empirical research of proposed cybersecurity management model and description of the sequence of research methods and procedures. The first and second section describes the prerequisites and principles for developing a conceptual cybersecurity management model, as well as a preliminary structure for the cybersecurity management model. The third and fourth section presents the research methodology of the proposed cybersecurity management model used in the organization of the empirical research and explains the criteria for the selection of experts.

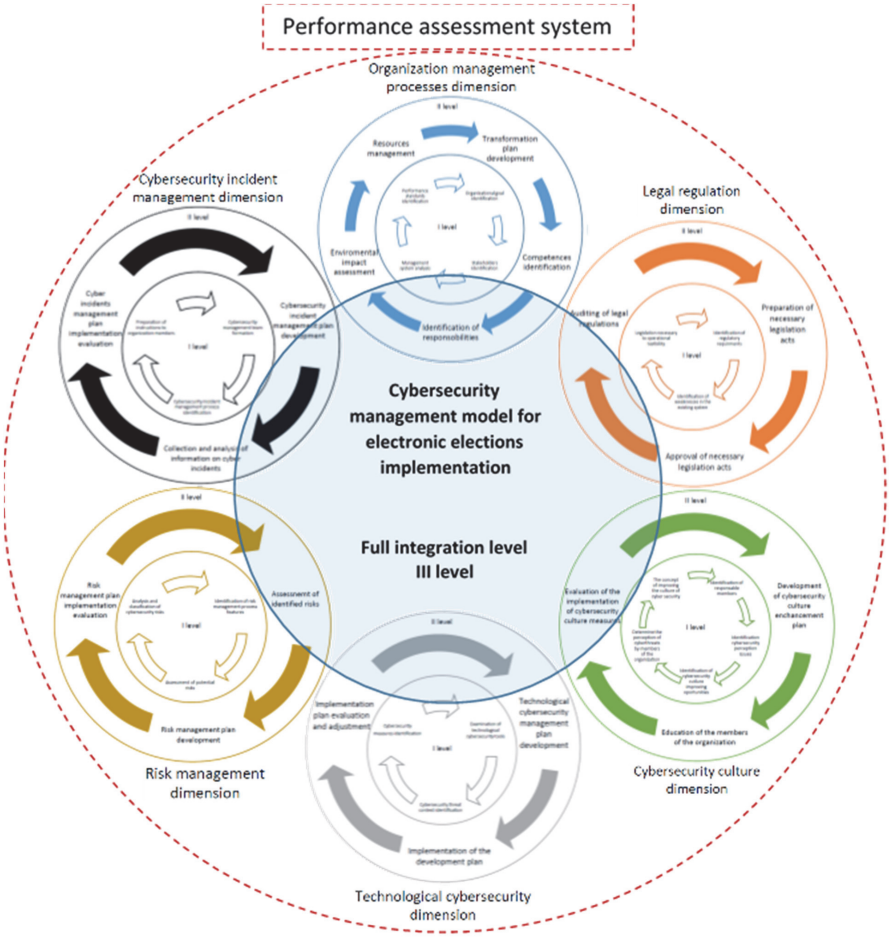
For the empirical study, a semi-structured interview method was selected, in which 9 cybersecurity experts were interviewed. It should be emphasized that the provision of technological cybersecurity cannot be considered as a sufficient means of ensuring cybersecurity in an organization. That reasoned that the proposed cybersecurity management model is technologically neutral. Also, in order to avoid a purely technology-based approach to cybersecurity, the researcher selected experts whose cybersecurity knowledge and experience is not only connected to the use of technological aspects of cybersecurity, but also to the development of cybersecurity policies, legal regulation, strategic cybersecurity planning. This method of selecting respondents ensures that the experts selected will not only be familiar with the solutions of the technological cybersecurity problem, but will also be aware of and experienced in other areas of cybersecurity. These abovementioned expertise and practical experience in cybersecurity suggest that the results of the empirical study will be reliable and comprehensive.

PART THREE OVERVIEW: CYBERSECURITY MANAGEMENT MODEL FOR ELECTRONIC VOTING IMPLEMENTATION EMPIRICAL RESEARCH RESULTS AND STRUCTURE ANALYSIS

The third part of the thesis is devoted to discuss and summarize the results of the empirical study of the proposed cybersecurity management model. Following the empirical research the results and the expert suggestions were used to refine the conceptual cybersecurity management model with the additional elements necessary to ensure a comprehensive cybersecurity management process during the implementation of electronic voting.

In this part of the dissertation the structure analysis of the revised cybersecurity management model is also carried out. After summarizing the results of the empirical study of the cybersecurity management model, the conceptual initial cybersecurity management model is supplemented with performance enhancing elements (see Fig. 2).

It is noteworthy that one of the six dimensions considered in the cybersecurity management model cannot be pointed out as the implementation of all six cybersecurity management dimensions in the organization and merging these dimensions into a single cybersecurity management system can show clear results of cybersecurity process change. Each dimension of the model can be developed separately, with different implementation times for the first and second levels, depending on the specifics of the organization, the resources managed, the resources available and the financial capabilities. However, it should be noted that the third level of all dimensions of the cybersecurity management model is related to the transformation of individual and interdependent organizational cybersecurity management processes (dimensions) into an integrated cybersecurity management system, the components of which are uniquely linked and interact.



Source: *created by the author according to Limba, Agafonov et al., 2017*

Fig. 2. *Cybersecurity management model for electronic elections implementation*

CONCLUSIONS AND RECOMMENDATIONS

1. The analysis of scientific sources, identifying theoretical aspects of cybersecurity management and the main causes and features of cybersecurity incidents, the problems of cybersecurity management and the possible impact of cybersecurity incidents on cybersecurity systems, reveal that:
   1.1. The variety of definitions implies problems of understanding this phenomenon, not only among those who are not directly exposed to the phenomenon on a daily basis, but also among those who are directly involved in cybersecurity challenges. The evolution of information technology-related security terms over the last three decades has led to various assumptions regarding the interpretation of the current cybersecurity term. Modern cybersecurity should be seen not only as a technological discipline but as an interdisciplinary phenomenon that addresses the technical, legal, personnel and organizational management and other sciences;
   1.2. The increasing penetration of information and communication technologies and their impact on various spheres of public life are creating conditions for the growth of cybersecurity threats and the number of successful cyber attacks;
   1.3. Organizations' trust in to the existing security tools and infrastructure, the personnel knowledge of information systems, the technology used and the functions it performs, and the misunderstanding of the surrounding environment create opportunities for successful cyberattacks against organizations and systems;
   1.4. Not only are the types of cybersecurity incidents and threats changing in today's technology-driven world, but the means of attack used are also improving. New types of attacks are emerging which purpose is not directly to use technological means to discredit information systems or the services they provide;
   1.5. Although technological cybersecurity vulnerabilities are considered to be one of the most important types of security vulnerabilities in the modern world, in the current period, the human factor is increasingly being identified as the reason for the most successful cyber attacks. Usage of technology tools and their automation, combining it with minimization of the human factor impact is essential to protect information resources from cyber threats;
   1.6. The first theoretical part of the dissertation focuses on the organizational cyber security management models used in the world, mainly focusing on the technological cybersecurity management in the organization, however, the models do not fully neglect the organizational, human resources, risk and incident management aspects;
   1.7. After conducting an analysis of cybersecurity incidents, attacks and potential vulnerabilities in the context of electronic election systems, the thesis presents a taxonomy of cybersecurity incidents in electronic voting;

1.8. The development and application of a management system in the process of designing electronic voting systems can provide the opportunity to eliminate most of the vulnerabilities identified and discussed in the dissertation.

2. The development of a conceptual cybersecurity management model based on theoretical insights that can be applied to the processes of design, deployment, management, and use of electronic election systems has revealed that:
   2.1. Six dimensions of cybersecurity model need to be addressed in order to properly manage cybersecurity in an organization: organizational governance processes, legal regulation, cybersecurity culture, technological security, risks and incident management;
   2.2. Managing cybersecurity threats through the implementation of these dimensions can help an organization successfully control potential risks and vulnerabilities and reduce the impact of successful cyber attacks;
   2.3. The biggest challenge is related to the integration of technological knowledge and management processes, as most aspects of cybersecurity management are often treated differently by technical staff and management professionals;
   2.4. Organizational change in the context of cybersecurity begins when security in an organization begins to be viewed not just as a technological discipline, but as a real challenge for the management system change;
   2.5. The cybersecurity management model also enables the organization's leaders to play an active role in decision-making and cybersecurity policy development, and enables the organization to properly assess security risks and mitigating measures;
   2.6. Implementing a cybersecurity management model also enhances an organization's external reputation by making the organization that cares about its cybersecurity more attractive to users or business partners;
   2.7. The idea and relevance of the proposed cybersecurity management model are connected to the development of a new approach to cybersecurity as it applies to the business processes of the entire organization, and each member of the organization must participate in the cybersecurity improvement;
   2.8. It is impossible to isolate an organization from the world and the cyber threats that exist within it and the cybersecurity management model must address not only the internal environment of the organization but also its interaction with the external environment.

3. An evaluation of the cyber security management model proposed in the empirical study and a summary of the results of the semi-structured expert interviews showed that:
   3.1. The components of the proposed cybersecurity management model: dimensions of organizational governance, legislation, cybersecurity culture, technology security, risk, and incident management, must be used to develop the cybersecurity management;

3.2. The proposed performance evaluation system, enables the organization to monitor changes in the implementation process in specific dimensions, as well as to identify the evolution process of the organization's cybersecurity management change;
3.3. Implementation of the proposed cybersecurity management model should be done in stages;
3.4. The influence of the dimension of organizational governance processes on the development of security within an organization can be described as a crucial process of implementing cybersecurity management model. Adjusting the organization's operations and adapting them to cybersecurity processes changes the organization's business model and opens up opportunities for vulnerability reduction;
3.5. Legislation aspects are inseparable from cybersecurity management. Within this dimension, the establishment of an organization's legal framework should be ensured enabling the organization to administratively increase the resilience of its internal environment to cyber threats;
3.6. By implementing the legislation dimension, the organization also has the ability to influence not only the internal but also the external environment by participating in the development of the state cyber security legal framework;
3.7. In order to reduce the vulnerability and to prevent cyber incidents, training and education of all employees, regardless of their position, is mandatory without exception. Such an integrated approach allows the elimination of potential threats (attacks), regardless of the type of personnel they are targeted at;
3.8. In cooperation with partners, service providers and other organizations, it is necessary to evaluate the cybersecurity level of potential partners, thus enabling them to avoid compromising their infrastructure and potential losses;
3.9. Technological cybersecurity should not be related to the selection of specific technological solutions, but rather as a technology-neutral process for managing equipment and cybersecurity solutions (tools), providing for the necessary actions of the organization to ensure business continuity and equipment life cycle support, resource planning, etc.;
3.10. Only proper risk assessment, classification, and identification of mitigation measures enable the organization to identify a strategy for avoiding or reducing potential vulnerabilities by balancing and minimizing the financial resources allocated to the process;
3.11. Managing cyber incidents within an organization should not be understood as responding to or mitigating a cyber attack, but as a continuous process that evaluates not only the internal infrastructure managed by the organization, but also the external environment: trends in cyber incident development, methods and techniques, alternatives to technological attacks, etc.;
3.12. Development of a cybersecurity culture, not only within the organization but across the state, can be the cause of the global improvement in cybersecurity,

but these skills should be developed at all levels, starting with primary education programs;

3.13. Possibility to create a secure electronic voting system depends on ability to convince the users (citizens) of this system that votes cast by the technology-based electoral system will not be falsified and the results of the elections will not be manipulated;

3.14. It is necessary to properly inform the public in order to form a proper public opinion on electronic elections. Public opinion formation, involving civil society organizations, state and local government representatives, media, cyber security experts and other stakeholder groups, can increase public confidence in electronic voting and speed up the implementation of this system, which is particularly relevant in the current pandemic times.

Scientific publications

1. Limba T.; Plėta T.; Agafonov K.; Damkus M., 2017. Cyber security management model for critical infrastructure, Entrepreneurship and Sustainability Issues 4(4): p. 559-573.
2. Limba, T.; Agafonov, K.; Paukštė, L.; Damkus, M.; Plėta, T. 2017. Peculiarities of cyber security management in the process of internet voting implementation, Entrepreneurship and Sustainability Issues 5(2): 368-402.
3. Plėta, T.; Tvaronavičienė, M.; Casa, S. D.; Agafonov, K. 2020. Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases, Insights into Regional Development 2(3): p. 703-715, <https://doi.org/10.9770/IRD.2020.2.3(7)>.

Presentations at scientific conferences

4. Agafonov K., Limba T., Damkus M. *Cyber Security: From Technology to Management.* Social Innovations: Theoretical and Practical Insights, 16th International Interdisciplinary Conference on Social Innovations, September 2016, Vilnius, Lithuania.
5. Agafonov K., Limba T., Plėta T., Damkus M. *Cyber Security Management in Internet Voting process.* Communication and Information Sciences in Networked Society: Experiences and Insights IV, 14-15 June 2018, Vilnius, Vilnius University.

CURRICULUM VITAE

Personal information

Name, Surname	Konstantin Agafonov
E-mail	ka1979@gmail.com

Education

2015 – 2021	Doctoral student at Mykolas Romeris University
2006 – 2008	Public administration master degree, Mykolas Romeris University
1997 – 2001	Informatics bachelor degree, Klaipeda University

Work experience

From 2005	National Defense system, officer
2008 – 2012	Mykolas Romeris University, lecturer
2004 – 2005	Klaipeda city Curonian secondary school, computer administrator
2003 – 2004	JSC „Technolitika“, manager-engineer
2002 – 2003	SC „Laivitė“, informatics engineer
2001 – 2002	JSC „Skaidula“, manager

Agafonov, Konstantin

KIBERNETINIO SAUGUMO VALDYMO MODELIS ELEKTRONINIAMS RINKIMAMS ĮGYVENDINTI: daktaro disertacija. – Vilnius: Mykolo Romerio universitetas, 2021. P. 234.

Bibliogr. 169–187 p.

Šiuolaikinė visuomenė yra stipriai priklausoma nuo kibernetinės erdvės ir jos saugumo. Valstybės, naudodamos technologijas, bando diegti elektroninius balsavimus ir taip priartinti piliečius prie šalies valdymo ir tiesioginio dalyvavimo politiniuose procesuose, bet nors pasaulis ir pasiekė labai aukštą technologinį išsivystymo lygį, jis vis dar nėra saugus kibernetinio saugumo kontekste. Kibernetinio saugumo užtikrinimas elektroninių rinkimų sistemų konstravimo ir naudojimo procese yra vienas iš svarbiausių aspektų, leisiančių sėkmingai įdiegti Lietuvoje elektroninių rinkimų sistemas. Apibendrinus apžvelgtos literatūros šaltinius ir empirinio tyrimo metu gautus rezultatus yra sukurtas kibernetinio saugumo valdymo modelis taikytinas elektroninių rinkimų įgyvendinimui. Sukurto kibernetinio saugumo valdymo modelio įdiegimas suteiks galimybę sėkmingai įgyvendinti elektroninius rinkimus, o taip pat užtikrins jų saugumą.

Modern society is heavily dependent from cyberspace and cybersecurity. Governments and States are using technology to push e-voting systems into citizen's lives in order to involve them in political processes. But although the world has reached a very high level of technological development, it is still not secure in the context of cybersecurity. Ensuring cybersecurity in the process of designing and operating electronic voting systems is one of the most important aspects for successful implementation of electronic voting in Lithuania. After summarizing the reviewed literature and the results obtained during the empirical research, a cybersecurity management model for the implementation of electronic voting systems was created. The implementation of the cybersecurity management model that has been created in this doctoral thesis will ensure successful implementation and cybersecurity of electronic voting systems.

Konstantin Agafonov

KIBERNETINIO SAUGUMO VALDYMO MODELIS
ELEKTRONINIAMS RINKIMAMS ĮGYVENDINTI

Daktaro disertacija
Socialiniai mokslai, vadyba (S 003)

Mykolo Romerio universitetas
Ateities g. 20, Vilnius
Puslapis internete www.mruni.eu
El. paštas roffice@mruni.eu
Tiražas 20 egz.

Parengė spaudai leidykla „Žara“

Spausdino UAB „Šiaulių spaustuvė“
P. Lukšio g. 9G, 76200 Šiauliai
info@dailu.lt
http://siauliuspaustuve.lt