Rokas GRINCEVIČIUS

DAKTARO DISERTACIJA

KIBERNETINIO SAUGUMO VALDYMO GERINIMAS TAIKANT ATSPARUMO MODELIUS ORGANIZACIJOSE

SOCIALINIAI MOKSLAI,
VADYBA (03 S)
VILNIUS, 2019

MYKOLO ROMERIO UNIVERSITETAS

MYKOLO ROMERIO UNIVERSITETAS

Rokas Grincevičius

KIBERNETINIO SAUGUMO VALDYMO GERINIMAS TAIKANT ATSPARUMO MODELIUS ORGANIZACIJOSE

Daktaro disertacija
Socialiniai mokslai, vadyba (03 S)

Vilnius, 2019

Mokslo daktaro disertacija rengta 2012–2018 metais Mykolo Romerio universitete pagal Vytauto Didžiojo universitetui su Klaipėdos universitetu, Aleksandro Stulginskio universitetu, Mykolo Romerio universitetu ir Šiaulių universitetu Lietuvos Respublikos švietimo ir mokslo ministro 2011 m. birželio 8 d. įsakymu Nr. V-1019 suteiktą doktorantūros teisę.

Mokslinė vadovė:
prof. dr. Aelita Skaržauskienė (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, 03 S)

ISBN 978-9955-19-936-6 (internete)
ISBN 978-9955-19-937-3 (spausdintinis)

TURINYS

SANTRUMPOS

angl. – sąvoka anglų kalba
APT – tikslinga ataka (angl. *advanced persistent threat*)
BYOD – asmeninės mobiliosios kompiuterijos įrenginiai naudojami darbui (angl. *bring your own device*)
CEO – vykdomasis direktorius (angl. *chief executive officer*)
CERT – saugos incidentų komanda (angl. *computer emergency readines team*)
CERT – reagavimo į kompiuterinio saugumo incidentus grupė (angl. *Computer Emergency Response Team*)
DB – duomenų bazė
DDoS – paskirstytas atsisakymas aptarnauti (angl. *denial-of-service attack*)
DMZ – demilitarizuota zona, tinklo perimetras (angl. *demilitarized zone*)
EK – Europos Komisija
ES – Europos Sąjunga
FNTT – Finansinių nusikaltimų tyrimo tarnyba
IDS – įsibrovimo nustatymo sistemos (angl. *intrusion detection*)
IPS – įsibrovimo prevencijos sistemos (angl. *intrusion prevention systems*)
IRT – informacinės ir ryšio technologijos
IS – informacinė sistema
IT – informacinės technologijos
JAV – Jungtinės Valstijos
JK – Jungtinė Karalystė
KAM – Lietuvos Respublikos krašto apsaugos ministerija
KST – Kibernetinio saugumo taryba
LKSĮ – Lietuvos kibernetinio saugumo įstatymas
LR – Lietuvos Respublika
NIST – Nacionalinis standartų ir technologijų institutas (angl. *National Institute of Standards and Technology*)
NKSC – Nacionalinis kibernetinio saugumo centras
NKSC/KSC – Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos
NSA – JAV nacionalinė saugumo agentūra (angl. *National Security Agency*)
PEF – Pasaulio ekonomikos forumas
RPO – sistemos duomenų praradimo masto susitarimas (angl. *recovery point objective*)
RRT – Lietuvos Respublikos ryšių reguliavimo tarnyba
RTO – sistemos neveikimo atsistatant susitarimas (angl. *recovery time objective*)
SLA – paslaugų lygio susitarimas (angl. *service level agreement*)
SOC – Saugumo operacijų sentras (angl. *Security Operations Center*)
STT – Lietuvos Respublikos specialiųjų tyrimų tarnyba
VK – Lietuvos Respublikos valstybės kontrolė
VMI – Valstybinė mokesčių inspekcija
VRK – Lietuvos Respublikos Vyriausioji rinkimų komisija
VRM – Lietuvos Respublikos vidaus reikalų ministerija
VSD – Lietuvos Respublikos valstybės saugumo departamentas
VT – valstybės tarnyba

PAVEIKSLŲ SĄRAŠAS

LENTELIŲ SĄRAŠAS

PRIEDŲ SĄRAŠAS

PAGRINDINĖS SĄVOKOS

Kibernetinis saugumas - darbe suvokiamas kaip yra apibrėžtas Lietuvos Respublikos kibernetinio saugumo įstatyme (2014), kuriame jis apibūdinamas kaip „[...] visuma teisinių informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei el. ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti“. Kibernetinio saugumo pagrindą sudaro trijų komponentų sąveika: **informacijos konfidencialumas** – informacijos apsauga nuo neteisėtos prieigos; **informacijos prieinamumas** – galimybė gauti reikiamą informaciją ar paslaugą per priimtiną laiką, būtent tuo momentu, kai jos reikia organizacijai; **informacijos vientisumas** – informacijos apsauga nuo nesankscionuoto pakeitimo, jos iškraipymo.

Kibernetinio saugumo valdymas - suvokiamas kaip informacinio saugumo valdymo bazinių principų evoliucija, nulemta kibernetinės erdvės plėtojimosi metu susiformavusio konteksto. Britanijos standartų institutas informacinio saugumo valdymą apibrėžia kaip „veiklos tęstinumo užtikrinimą bei žalos veiklai mažinimą, vykdant organizacijos informacinėms vertybėms grėsmę keliančių saugos incidentų prevenciją ir jų poveikio mažinimą“ (British Standards Institution, 1995). Pagal Craigen ir kt. (2014), šių procesų tikslas yra apsaugoti kibernetinę erdvę ir kibernetinėje erdvėje veikiančias sistemas nuo įvykių, kurių metu sąlygojamas neatitikimo atsiradimas tarp saugomų vertybių suvokiamų (de jure) ir faktinių (de facto) būsenų.

Kibernetinė erdvė - Lietuvos Respublikos kibernetinio saugumo įstatyme apibūdinama kaip „aplinka, kurioje pavieniuose kompiuteriuose ar kitoje informacinėje ir ryšių technologijų įrangoje sukuriama elektroninė informacija ir (arba) perduodama per elektroninių ryšių tinklu sujungtus kompiuterius ar kitą informacinių ir ryšių technologijų įrangą“ (LR kibernetinio saugumo įstatymas, 2014). JAV ginkluotųjų pajėgų jungtinis operacijų štabas (2013) kibernetinę erdvę apibrėžia kaip globalų domeną, bendroje informacinėje erdvėje, sudarytą iš nepriklausomų informacinių technologijų tinklų infrastruktūros: interneto, telekomunikacijų tinklų, kompiuterijos sistemų, įterptinių procesų ir valdiklių bei duomenų. Internetas yra kibernetinės erdvės dalis, jis nėra visa kibernetinė erdvė. Kiekvienas kompiuteris gebantis komunikuoti su kitu kompiuteriu ar kompiuterijos sistema, kiekvienas prie interneto prijungtas mobilios telefonijos įrenginys yra kibernetinės erdvės dalis (Bryant, 2015).

Kibernetinis atsparumas – gebėjimas adaptuotis prie kintančių sąlygų, atlaikyti griaunamuosius veiksmus juos absorbuojant ir greitai po jų atsistatyti (Bruneau ir kt., 2003; Gao ir kt., 2011; Sansavini ir Nan, 2017). Singer ir Friedman (2013) atsparumą suvokia kaip perspektyvų būdą patobulinti bendrą saugumo lygį.

ĮVADAS

Temos aktualumas. Įvairioms žmogiškoms veikloms persikeliant į elektroninę erdvę, taip pat vyksta ir tradicinio bei kibernetinio nusikalstamumo konvergencija, pašalinanti visas egzistuojančias ribas tarp fiziniais metodais vykdomų nusikalstamų veikų ir virtualių nusikaltimų. Atsiradus naujiems veiklos modeliams, nusikaltėliai atranda ir naujus nusikaltimo būdus, kuriuose elektroninės priemonės ir duomenys gali būti taikiniu arba atliekamo nusikaltimo įrankiu. Nusikaltimų, teroristinių išpuolių, pramoninio ir politinio šnipinėjimo vykdymo atvejų prieš fizinius asmenis, organizacijas, valstybes, kritinę infrastruktūrą kasmet vis daugėja. 2017 m. birželį įvykdyta didžiulio masto kibernetinė ataka nukreipta prieš verslo įmones, oro uostus, bankus ir valstybines institucijas Ukrainoje[1], kuri vėliau išplito ir kitose Europos valstybėse, tarp jų ir Lietuvoje. Tai buvo antroji ataka, po vos tik prieš kelias savaites įvykusios ir 150 valstybių paveikusios WannaCry atakos - nukreiptos ne tik prieš pavienes organizacijas, bet ir tokias svarbias funkcijas atliekančias sistemas, kaip Jungtinės Karalystės Nacionalinės sveikatos tarnyba. Jungtinės Karalystės gynybos sekretorius seras Michael Fallon netgi įspėjo už atakas atsakingą šalį, kad į ateities kibernetines atakas Jungtinė Karalystė galėtų atsakyti karinių oro pajėgų smūgiais ar netgi prieš jų rengėjus pasiųsti kariuomenę. Pasak sekretoriaus, tokie kibernetiniai išpuoliai „galėtų iššaukti atsaką iš bet kurio domeno – oro, žemės, jūros ar kibernetinės erdvės“[2]. Kibernetinės grėsmės reikalauja vis didesnių resursų naujų, adekvačių atsako formų paieškoms, sąlygoja sisteminius veiklos sutrikdymus ir milžiniškus finansinius nuostolius. Pagal Jungtinės Karalystės draudimo rinkos Lloyd's of London vertinimą, kibernetinės atakos verslui globaliai per vienerius metus kainuoja 400 milijardų JAV dolerių (Hubbard, Seiersen, 2016). Globali draudimo bendrovė XL Catlin, savo draudimo produktų linijoje siūlančioje ir galimybę apsidrausti nuo kibernetinių incidentų sukeltų nuostolių, kibernetines grėsmes įvardino didžiausiomis sisteminėmis grėsmėmis, kurias ji matė per visa savo daugiau nei 40 metų trunkančią praktiką draudimo versle (Z/Yen Group, 2015). Kibernetinės priemonės taip pat vis dažniau tampa geopolitinio konflikto instrumentu naujai besiformuojančių nekonvencinių priešpriešos formų kontekste. Kaip pažymi Rusijos generalinio štabo generolas Valerijus Gerasimovas, XXI a. karai daugiau nėra skelbiami, o blunkant riboms tarp karo ir taikos būsenų, konfliktams spręsti vis dažniau taikomos hibridinės priemonės, apimančios politinius, ekonominius, humanitarinius, informacinius ir kitus ne karinius metodus (Gerasimov, 2013). Šiuos teiginius Rusija praktiškai įgyvendino 2014 m. vykusios Krymo aneksijos metu, kai lygiagrečiai su skiriamųjų ženklų neturinčiomis specialiųjų pajėgų grupėmis, naudotomis užimti Ukrainos valstybines institucijas, organizavo kibernetines atakas prieš Ukrainos valstybinę logistinę ir informacinę infrastruktūrą, vykdė dezinformuojančius veiksmus socialiniuose tinkluose (Duggan, 2015). Esant tokiai situacijai bei atsiminus vienus ryškiausių pastarojo meto įvykius, kai kibernetinės priemonės buvo taikomos paveikti fizinėje erdvėje esančius procesus, pavyzdžiui, rinkimus JAV, sudėtinga būtų nesutikti su teiginiais, kad kibernetinis saugumas yra su valstybės suverenumu,

1 http://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1/

2 http://www.telegraph.co.uk/news/2017/06/27/cyber-attack-could-lead-military-retaliation-says-fallon/

nacionaliniu saugumu, kultūriniu paveldu bei gėrybėmis ir vertybėmis susijęs klausimas, atliekantis saugaus ekonominės plėtros garanto funkcijas (Ghernaouti, 2013). Atsižvelgiant į tai, kad nepaisant tęstinio rizikų valdymo progreso, kibernetinėje srityje visų potencialių atakų prognozavimas ir prevencija yra neįmanomas uždavinys dabartinėms ir netgi ateities kibernetinėms sistemoms (Linkov ir kt., 2013) bei tradicinių metodų, paremtų rizikų matricomis neveiksmingumą ir placebo įspūdžio sudarymą (Hubbard, Seiersen, 2016), būtina ieškoti būdų ir naujų požiūrių, kaip padaryti norimas apsaugoti sistemas atspariomis, galinčiomis absorbuoti kibernetines atakas, adaptuotis prie jų nuolatos keliamų iššūkių ir kuo greičiau po jų atsistatyti. Toks atsakas galėtų būti tarpdisciplininiu požiūriu paremti kibernetinio saugumo ir atsparumo valdymo tyrimai.

Mokslinė problema ir jos ištirtumo lygis. Nagrinėjant kibernetinio saugumo valdymo literatūrą, kurioje analizuojama kibernetinio atsparumo perspektyva, skirtinos kelios, šiam darbui aktualios teorinės iteracijos. Pirma – informacinių sistemų ir jose vykstančių procesų atsparumas, t.y. informacines sistemas veikloje naudojančių organizacijų atsparumas, dėl šių technologijų taikymo ir su jomis susijusių procesų vykdymo kylančioms grėsmėms. Antra – organizacijų, kaip visumos, atsparumas kibernetinėms grėsmėms. Vienas ankstyvesnių bandymų nagrinėti ir suprasti organizacijų atsparumą iš informacinių sistemų perspektyvos yra Riolli ir Savicki (2003) tyrimas, kurį patys autoriai pozicionuoja kaip atsaką į tuo metu šioje srityje buvusį teorinį vakuumą. Autorių darbas integruoja tuo metu egzistavusias individualaus, psichologinio ir organizacinio atsparumo teorijas. Nors šio tyrimo atveju įvardijamas sisteminis stresorius nėra kibernetinės organizacijai kylančios grėsmės, vertėtų akcentuoti tyrėjų išskirtus keletą svarbių faktorių, reikšmingų bendrojo kibernetinio atsparumo idėjų formavimui. Visų pirma, stresą organizacinei sistemai sukelia jos veiklos erdvėje egzistuojantys technologiniai pokyčiai, aukštas informacinių sistemų dinamikos laipsnis ir nuolatinė rinkų akceleracija. Antra, atsparumas būdamas sisteminiu faktoriumi, priklausomu nuo aibės organizacinės sistemos atributų, užtikrinamas tik individualiame lygmenyje negarantuoja visos organizacijos atsparumo. Būtina plėtoti abu lygius kaip visumą (Riolli, Savicki, 2003). Starr, Newfrock ir Delurey (2003), kalbėdami apie organizacijų atsparumą įtinklintos ekonomikos ir tinklinių organizacijų kontekste, akcentavo aibę atsparumo užtikrinimo faktorių, iš kurių skirtini: situacijos žinojimas, rizikų valdymas bei organizacijos struktūrinio sudėtingumo suvokimas. Starr, Newfrock ir Delurey (2003) pagrindiniu organizacinės sistemos stresoriumi įvardina bendrąsias rizikas, kylančias dėl tinklinėse struktūrose atsiradusių komunikacijos, tiekimo ir kitų sutrikimų. Milligan ir Hutcheson (2006) vertino informacinių technologijų teikimo taikant užsakomųjų paslaugų modelius (angl. *outsourcing*) įtaką organizacijos kibernetiniam atsparumui. Pažymėtina, kad Milligan ir Hutcheson (2006) tarp aibės kitų operacijų ir palaikymo rizikų išskiria ir loginio saugumo rizikas. Nors šios rizikos sudaro tik mažą bendrųjų organizacijos rizikų dalį, reikėtų akcentuoti, kad toks integruotas rizikų valdymas vertintinas, kaip pakankamai brandus rizikų valdymo požiūris. Kiek vėliau organizacijų atsparumą iš verslo valdymo sistemų perspektyvos nagrinėjo Ignatiadis ir Nandhakumar (2007). Vienas esminių tyrėjų teiginių yra toks: „Sudėtingos verslo valdymo sistemos dėl savo taikomų kontrolės mechanizmų yra rigidiškos prigimties, jos turi polinkį slopinti ir mažinti bendrąjį organizacijos lankstumą ir atsparumą“. Taip pat vertėtų išskirti Werfs ir Baxter (2013),

nagrinėjusių sociotechnines adaptyvias sistemas iš atsparumo perspektyvų, tačiau neakcentuojančių jų atsparumo būtent kibernetinėms grėsmėms.

Plėtojant diskusiją apie antrąją atsparumo tyrimų iteraciją, didžiausią aktyvumą įgavusią šio dešimtmečio pradžioje, reikia pažymėti, kad daugiausia dėmesio ją atstovaujantys tyrėjai skiria atsparumo metrikų formavimui bei atsparumo plėtojimui kritinės infrastruktūros sistemose; valdymo perspektyva kibernetinio atsparumo tyrimuose sutinkama ypač retai. Kalbant apie sisteminius kibernetinio atsparumo aspektus, vertėtų išskirti Goldman (2010), nagrinėjusios kritinių sistemų projektavimo, diegimo ir valdymo procesus iš atsparumo perspektyvos. Vienas esminių autorės teiginių yra raginimas suvokti, kad neįmanoma sustabdyti kibernetinių atakų, tačiau sistemų architektūros pertvarka taikant atsparumo požiūrius gali sumažinti atakos pasekmes, pakelti jų kainą puolančiajai pusei ir veikti kaip atgrasymo priemonė ateityje (Goldman, 2010). Kibernetinis atsparumas tyrinėtas ne tik kaip sisteminis elementas, bet ir kaip projektavimo objektas (Bodeau ir kt., 2012; Bodeau, Graubart, Laderman, 2014; Häring, Ebenhöch, Stolz, 2016; Sansavini, 2017). Literatūroje taip pat sutinkami bandymai tyrinėti kibernetinio atsparumo dinamiką skirtingose sisteminėse aplinkose: mažose verslo įmonėse (Williams ir Manheke, 2010), sveikatos apsaugos sektoriuje (Williams, 2010), debesų kompiuterijos sistemose (Thebeau ir kt., 2014), e. sveikatos sistemose (Liveri, Sarri ir Skouloudi, 2015), transporto srityje (Nogal ir O'Connor, 2017), elektros inžinerijoje (Zussblatt ir kt., 2017) tiekimo grandyse (Urciuoli, 2015), konkrečiuose geografiniuose ir politiniuose vienetuose (Kaufmann, 2015; Peter, 2017), politinio sudėtingumo perspektyvoje (Herrington ir Aldrich, 2013), organizacijos veiklos reputacijos išsaugojimo procesuose (Wilding, 2016). Taip pat vertėtų išskirti nemažą skaičių įvairių autorių suformuotų atsparumo matavimo modelių ir metrikų, skirtų išmatuoti organizacijos, sistemos, padalinio ar kito organizacinio vieneto atsparumą kibernetinėms grėsmėms (Wang ir kt., 2010; Allen, 2011; Ford ir kt., 2012; Linkov ir kt., 2013; Vugrin ir Turgeon, 2013; Houston ir Sicker, 2014; Bodeau ir Graubart, 2016; Friedberg ir kt., 2016; Shapiro, 2016; Häring ir kt., 2017; Heinimann ir Hatfield, 2017). Atskirai vertėtų pažymėti Tran ir kt. (2016) modelį, suformuotą įveikti nulinės dienos kenkėjiškos programinės įrangos keliamus iššūkius. Kalbant apie kibernetinio atsparumo tyrimus kritinės infrastruktūros sistemose, atsparumas šioje perspektyvoje nagrinėtas kaip nacionalinės ir korporatyvios socialinės atsakomybės elementas (Ridley, 2011), kompleksiškų kritinių infrastruktūrų sistemų pagrindas (Lewis, Mackin, Darken, 2011), kritinės infrastruktūros komponentas iš sociopolitinės ir procedūrinės perspektyvų (Lundborg ir Vaughan-Williams, 2011; Moteff, 2012), kaip pramonės procesų valdymo sistemų elementas (Krotofil ir Cárdenas, 2013; Chaves ir kt., 2017), kaip kritinės infrastruktūros absorbavimo, adaptavimosi ir veiklos atstatymo pagrindas (Setola, Luiijf, Theocharidou, 2016; Balutis ir kt., 2016), kritinės infrastruktūros socialinio atsparumo elementas (Trump ir kt., 2017), kritinės infrastruktūros viešojo ir privataus sektoriaus partnerystės objektas (Trucco ir Petrnej, 2017), konkrečios valstybės kritinės infrastruktūros apsektas (Todorovic ir kt., 2017).

Dėl egzistuojančio tyrimų fragmentiškumo ir suvokimo problematikos sudėtinga apibrėžti, kur baigiasi vienų organizacinių kibernetinio saugumo valdymo atsakomybių ribos ir prasideda kitų. Tai suformuoja būtinybę išgryninti esamą kibernetinio saugumo sąvokų terminiją ir nustatyti konceptualias kiekvieno šio reiškinio vartosenos ribas. Nagrinėjant

mokslinę literatūrą, teisės aktus, NATO ir ES bei aukščiausio lygmens politikų pasisakymus, galima teigti, kad bendroje kibernetinio saugumo valdymo technologinių komponentų aibėje kibernetinis atsparumas yra viena reikalingiausių šių laikų sociotechninių sistemų savybių, tačiau nėra pakankamai aišku, kokiomis priemonėmis ši savybė turėtų būti įgyvendinama, palaikoma ir didinama. Akivaizdu, kad kibernetinio atsparumo konceptualaus suvokimo ir įgyvendinimo principai skirtinguose sociotechniniuose junginiuose gali būti plėtojami skirtingai, įvertinant konkrečiame vienete egzistuojančią organizacinę kultūrą ir valdymo tradicijas. Visus šiuos teiginius galima apibendrinti **moksline problema**, išreiškiamą klausimu: „Kaip formuoti kibernetinio saugumo valdymo procesus, siekiant pagerinti organizacijų atsparumą kibernetinėms grėsmėms?“.

Tyrimo objektas – organizacijų kibernetinio saugumo valdymo gerinimas.

Tyrimo tikslas – suformuoti validuotą kibernetinio saugumo valdymo modelį paremtą atsparumo požiūriu.

Tyrimo uždaviniai:

1. Atlikus mokslinių šaltinių analizę atskleisti kibernetinių grėsmių dinamiką, kibernetinio saugumo ir atsparumo objektą, kibernetinio atsparumo valdymo aspektus, formavimo prielaidas ir kliūtis, identifikuoti esminius faktorius lemiančius kibernetinio saugumo aktualizavimą skirtinguose organizacijos valdymo lygmenyse.
2. Teorinių įžvalgų pagrindu suformuoti konceptualų kibernetinio saugumo valdymo modelį, integruojantį svarbiausius organizacijų kibernetinio atsparumo sisteminius ir valdymo faktorius.
3. Validuoti konceptualųjį kibernetinio saugumo valdymo modelį ir nustatyti svarbiausius jo konstrukcinius elementus, atliekant pusiau struktūrizuotą kibernetinio saugumo ekspertų interviu bei kokybinę Lietuvos kibernetinį saugumą reglamentuojančių teisės aktų analizę.
4. Modelio pagrindu pateikti praktines rekomendacijas, kaip galėtų būti gerinamas kibernetinio saugumo valdymas organizacijose taikant kibernetinio atsparumo požiūrius.

Ginamieji teiginiai:

1. Kibernetinio saugumo tyrimų ir praktiniuose domenuose susiduriama su kibernetinio saugumo valdymo sampratos problematika, todėl būtinas šios srities terminijos išgryninimas, sąvokų suvienodinimas, kibernetinio saugumo praplėtimas sistemine ir valdymo perspektyvomis.
2. Kibernetio saugumo valdymo gerinimas neatskiriamas nuo bendro saugumo bendruomenės kibernetinio raštingumo lygio augimo, kibernetinio saugumo sistemos veikėjų gebėjimo keistis informacija procesų tobulinimo, tarpinstitucinio bendradarbiavimo skatinimo įvairiuose organizacinių sistemų valdymo lygmenyse.
3. Didėjant kibernetinių atakų skaičiui ir augant jų sudėtingumo lygiui, viena aktualiausių sistemos savybių tampa atsparumas, todėl skatintinas atsparumo požiūriu paremtas kibernetino saugumo valdymas. Kibernetinio saugumo valdymas tobulintinas taikant parengtą kibernetinio saugumo valdymo gerinimo modelį.

4. Kibernetinio atsparumo plėtra organizacijose sąlygoja bendrąją organizacijos, kaip sociotechninės sistemos, evoliuciją, didina sistemos teikiamų paslaugų gavėjų pasitikėjimą sistema.

Disertacinio darbo tyrimo metodai:

Teoriniai metodai. Siekiant suformuoti kibernetinio saugumo valdymo modelio teorinį pagrindą buvo vykdoma mokslinės literatūros analizė, kurios metu taikyti sisteminimo, sintezės, lyginimo bei apibendrinimo metodai. Modelio suformavimui taikyti konceptualiojo modeliavimo ir vizualizacijos metodai.

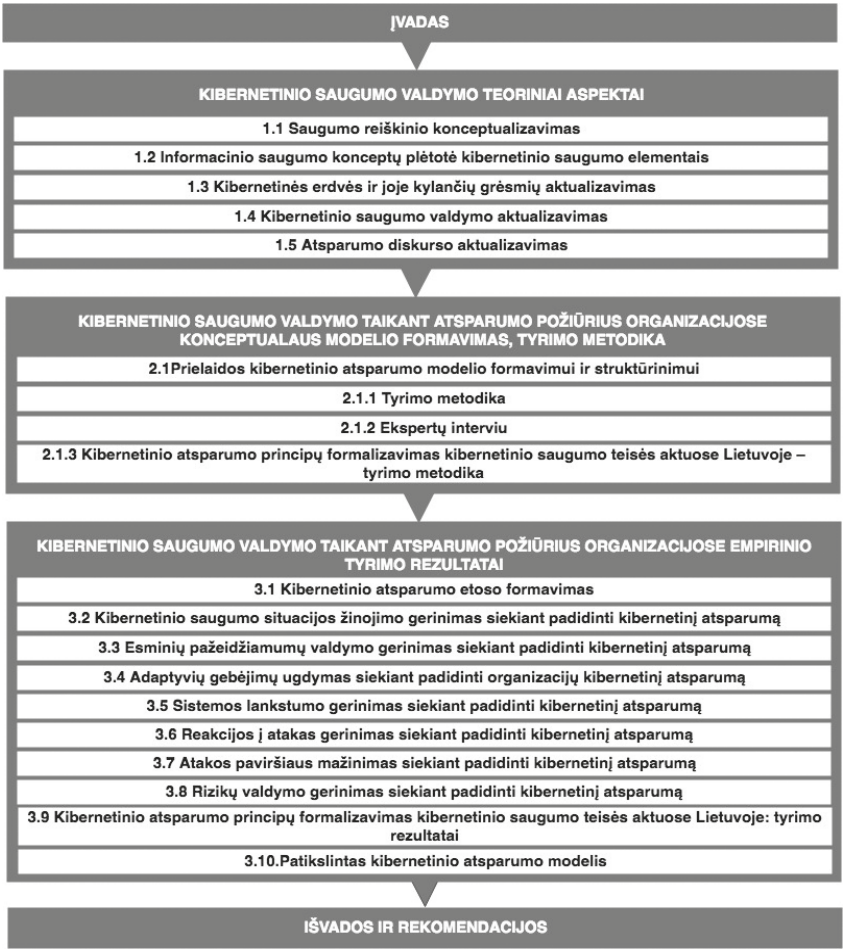
Empiriniai metodai. Modelio validacijai taikyti vienas kitą papildantys kokybiniai empiriniai tyrimai: ekspertinis interviu, kokybinė turinio analizė, antrinių šaltinių duomenų analizė.

Mokslinė darbo vertė ir mokslinis darbo naujumas. Darbe taikant tarpdisciplininį, holistinį požiūrį praplėstas egzistuojantis kibernetinio saugumo valdymo ir atsparumo tyrimų diskursas, įtraukiant į jį organizacinius ir valdymo aspektus. Darbe išgrynintos kibernetinio atsparumo suvokties ribos, išskirti pagrindiniai organizacijų kibernetinio atsparumo elementai. Organizacijų atsparumas kibernetinėms grėsmėms išnagrinėtas keliais valdymo lygmenimis, taip sudarant prielaidas tolimesnei kibernetinio atsparumo procesų ir jų metu vykdomų sąveikų analizės plėtotei. Darbu daromas mokslinis indėlis į bendrą kibernetinio saugumo valdymo tyrimų lauką, formuojamos prielaidos tolimesniam reiškinio tyrinėjimui.

Praktinė darbo reikšmė. Darbas atskleidžia egzistuojančias kibernetinio saugumo valdymo problemas ir pasiūlo priemones joms spręsti, taikant atsparumu paremtus požiūrius ir tokiu būdu pagerinant kibernetinio saugumo valdymą viešojo sektoriaus organizacijose Lietuvoje. Nuolatos vis dažnėja raginimai didinti sistemų atsparumą kibernetinėms grėsmėms, tačiau praktiškai nėra metodikų, aprašančių, kaip šie procesai turėtų būti įgyvendinami. Suformuotas organizacijų kibernetinio saugumo modelis taikytinas plėtojant kibernetinio atsparumo iniciatyvas organizacijose įvairiuose valdymo lygmenyse.

Reikšminiai žodžiai: informacinis saugumas, kibernetinis saugumas, kibernetinio saugumo valdymas, kibernetinis atsparumas, kibernetinės grėsmės, atsparumo modelių taikymas kibernetinio saugumo valdymui gerinti.

Disertacinio darbo struktūra. Disertacinio darbo struktūra, kuri yra grindžiama tyrimo tikslu ir uždaviniais, pateikiama 1 paveiksle.



Šaltinis: *parengta autoriaus*

1 pav. *Disertacijos loginė struktūra*

Pirmojoje teorinėje disertacijos dalyje nagrinėjama saugumo reiškinio transformacija, atskleidžiama, kas sąlygojo poreikį konceptualiai permąstyti informacinio saugumo reiškinį bei ieškoti naujų, valdymo elementus integruojančių kibernetinio saugumo veiklų organizavimo būdų. Apžvelgiama kibernetinėje erdvėje kylančių grėsmių dinamika, įvertinama kibernetinio saugumo valdymo metodų kaita bei naujų, atsparumu pagrįsto valdymo požiūrių taikymo poreikis. Antrojoje disertacijos dalyje aprašoma atlikto empirinio tyrimo ir pasirinktų Lietuvos Respublikos kibernetinį saugumą reglamentuojančių teisės aktų tyrimo metodika. Trečiojoje darbo dalyje pateikiami atlikto empirinio tyrimo rezultatai ir validuotas kibernetinio saugumo valdymo taikant atsparumo požiūrius konceptualus modelis, integruojantis esminius organizacijos kibernetinio atsparumo užtikrinimo elementus.

1. KIBERNETINIO SAUGUMO VALDYMO TEORINIAI ASPEKTAI

Šios tyrimo dalies paskirtis yra žvalgomoji; jos metu norima pasiekti dalį esminių, žvalgomiesiems tyrimams būdingų uždavinių:

- susipažinti su tiriamojo reiškinio faktine situacija, nustatyti egzistuojančius trūkumus;
- suformuoti bendrinį mentalinį esamos situacijos paveikslą (Neuman, 2007).

Žvalgomasis požiūris pasirinktas atsižvelgiant į siekį geriau suvokti nagrinėjamą kibernetinio atsparumo reiškinį, kuris yra pakankamai naujas, o lietuviškame kontekste apskritai nenagrinėtas. Taikant žvalgomąjį požiūrį, bandoma atsakyti į klausimą: „Kas?“. Šioje disertacijoje: „Kas yra organizacinis atsparumas kibernetinėms grėsmėms?“. Pagal Neuman (2007), viena esminių žvalgomojo tyrimo dalių – **konceptualizacija**, kuri yra konkretaus konstrukto išgryninimas, suteikiant jam konceptualų ar teorinį apibrėžimą, formuojamą remiantis įvairias egzistuojančiais šaltiniais: asmenine tyrėjo patirtimi, kruopščiai atliekamu giluminiu mąstymu, diskusijomis su srities ekspertais, esama moksline literatūra (Neuman, 2007). Kitas svarbus tyrimo elementas – **operacionalizacija**, kurią atliekant sukuriamos sąsajos tarp konceptualių apibrėžimų ir konkrečios aibės matavimo technikų ir procedūrų. Operacionalizacija susieja teoriją, kuri yra kupina abstrakčių konceptų, prielaidų, priežastinių ryšių ir apibrėžimų su empiriniais matavimais, kurie apibrėžia konkrečiai pamatuojamus kintamuosius (Neuman, 2007), kitaip tariant, tyrėjas formuoja konceptualius apibrėžimus iš pradinių darbinių idėjų ir vėliau paaiškina, kaip tam tikri stebėjimai ir mintys padeda susiformuoti darbinėms idėjoms.

1.1. Saugumo reiškinio konceptualizavimas, saugumo objektų apibrėžties problematika

Veikiausiai, vienokio ar kitokio pobūdžio susidomėjimas informacijos saugumu egzistuoja tiek pat, kiek ir pati informacija, o atsiradus kompiuterizuotoms informacijos apdorojimo ir perdavimo priemonėms, dėmesys informaciniam saugumui dar labiau išaugo ir perkėlė šį tyrimų domeną į visiškai kitokį lygį. Nepaisant to, informacinio saugumo tyrimų sritis turi gan aukštą problematikos lygmenį. Kaip šio amžiaus pradžioje pastebėjo Kotulic ir Clark (2004), atkreipę dėmesį į empirinių tyrimų trūkumą saugumo rizikos valdymo srityje, informacinio saugumo tyrimai yra laikomi vienais skvarbiausių organizacinių tyrimų rūšių, todėl egzistuoja bendrinis nepasitikėjimas bet kokiais pašaliečių bandymais gauti duomenis iš organizacijos apie jos taikomus saugumo sprendimus, kai egzistuoja grėsmė organizacijos saugumui, saugos praktikų bendruomenė yra jokiais būdais nelinkusi atskleisti „jautrios“ informacijos. Willison ir Siponen (2007) taip pat daro prielaidą, kad informacinės saugos tyrimų laukas yra teoriškai nepakankamai išplėtotas ir, nors kibernetinių nusikaltimų skaičius auga, tyrimų augimas išlieka pakankamai žemas. Kaip pažymi Kenneally ir Bailey (2013), vienas pagrindinių kibernetinio saugumo tyrimų lauko iššūkių yra balansavimas ant etiškumo ribos. Informacinis saugumas yra ganėtinai uždara disciplina, kurios vystymasis ne visuomet vyksta sinchroniškai kartu su kitais IRT srities komponentais (Rao ir Nayak, 2014).

Prieš vykdant gilesnę kibernetinio saugumo analizę, vertėtų panagrinėti bandymus konceptualizuoti informacinių technologijų srityje vykdomus saugumo užtikrinimo procesus. Pažymėtina, kad ilgą laiką šioje srityje vyravo informacinio saugumo sąvoka. Informacinis saugumas, vertinat jį iš terminijos perspektyvų, yra ganėtinai problematiškas reiškinys. Visų pirma todėl, kad neturi aiškios, nuoseklios apibrėžties – literatūroje ir praktikoje pakankamai ilgai dominavo kompiuterių saugumo, informacinių sistemų saugumo, elektroninės informacijos saugumo sąvokos. Antra, ilgą laiką informacinio saugumo laukas buvo papildomas tokiais reiškiniais kaip informacijos užtikrinimas (angl. *information assurance*). Galiausiai, pradėjus naudoti vėlesniam laikotarpiui būdingus saugumo terminus, ankstesnieji apibrėžimai nebuvo visiškai išstumti iš vartosenos ir vis dar yra dažnai sutinkami tiek literatūroje, tiek praktikoje, dažnai kartu su šiomis ilgainiui nusistovėjusiomis sąvokomis taikant ir tipinius dabartinio saugumo laikotarpio terminus, tokius kaip: kibernetinis incidentas, kibernetinė grėsmė, o pastaruoju metu, tam tikrose saugumo bendruomenėse – ir skaitmeninis saugumas. Tai sąlygoja tam tikrą terminų sąmyšį, kuris pastebimas nagrinėjant tiek saugumo srities literatūrą bei įvairių saugumo organizacijų ir valstybinių institucijų parengtas baltąsias knygas ar kitokios formos ataskaitas, tiek skirtingų šalių informacinių sistemų saugumą reglamentuojančius teisės aktus.

Plėtojant saugumo suvokimo problematiką, pažymėtina, kad sudėtinga informacinio saugumo konceptą vertinti ir iš elektroninėje erdvėje įvykdomų nusikaltimų perspektyvos. Nepaisant to, kad pagal Europolo vertinimą[3] - kibernetinis nusikalstamumas yra viena sparčiausiai augančių nusikalstamumo rūšių, neretai vis dar pasigendama vieningo apibrėžimo, apibūdinančio kas yra neteisėta veikla internete. Kaip pažymi Sherwood, Clark ir Lynas (2005), kadangi nėra absoliučios saugumo ir nesaugumo matavimo skalės, saugumas yra reliatyvi sąvoka ir įgauna prasmę tik tuomet, kai saugos objektui suteikiama visuotinai pripažįstama vertė ir dėl šiam objektui kylančio potencialaus pavojaus jį būtina apsaugoti. Toks objektas organizaciniame kontekste yra įvardinamas kaip vertybė, kurią sunaikinus arba pasisavinus organizacija patiria neigiamą poveikį, todėl kiekvienas saugos veiksmas visų pirma turėtų būti derinamas su organizacijos poreikiais (Sherwood, Clark, Lynas, 2005). Bandant konkretizuoti ir nagrinėti informacinį saugumą iš sisteminės perspektyvos vertėtų išskirti Landwehr ir kt. (2001) akcentuojamą sistemos saugumo sampratą, pagal kurią, tyrėjai saugia sistema laiko tokią, kurioje nuo neautorizuoto atskleidimo, modifikavimo ir išsigynimo (angl. denial) yra adekvačiai apsaugoma joje apdorojama informacija. Pasak Landwehr ir kt. (2001), adekvatumą būtina išskirti, nes nei viena praktiškai egzistuojanti sistema negali besąlygiškai užtikrinti visiško saugumo būsenos, todėl iš savo prigimties saugumas yra reliatyvus, ypač nuo konteksto priklausomas reiškinys ir įgauna visiškai kitokią prasmę aukštųjų karo technologijų kontekste, lyginant ją su nedidele, pavyzdžiui, prekybine organizacija (Stahl, Shaw, Doherty, 2008). Nepaisant egzistuojančio sveiko proto padiktuoto, bendrai sutariamo suvokimo apie saugumą, kartais organizacijų vykdoma veikla nėra lemiamas faktorius ir nedidelės, jokios kritinės veiklos nevykdančios organizacijos yra pakankamai apsaugojusios savo elektroninius resursus, o aukštą formalizavo lygmenį turinčiose ir gerai finansuojamose sistemose saugumas gali išlikti nepakankamas (Landwehr, 1981). Apibendrinant anksčiau išsakytus teiginius, konstatuotina,

3 https://www.europol.europa.eu/sites/default/ les/publications/iocta.pdf

kad nepriklausomai nuo konkretaus taikytino informacinio saugumo apibrėžimo, **būtina identifikuoti saugumo objektą, suteikti jam visuotinai pripažįstamą vertę ir adekvačiomis priemonėmis jį apsaugoti**. Šiuolaikinėse organizacijose toks saugumo objektas dažniausiai yra informacija, kuris yra viena svarbiausių jos vertybių (Hong ir kt., 2003), tad priklausomai nuo jos svarbos organizacijai, nustatomas jai perduoti, apdoroti ir kitus su šios informacijos valdymo veiksmais atlikti skirtos infrastruktūros saugumo priemonių adekvatumo lygmuo.

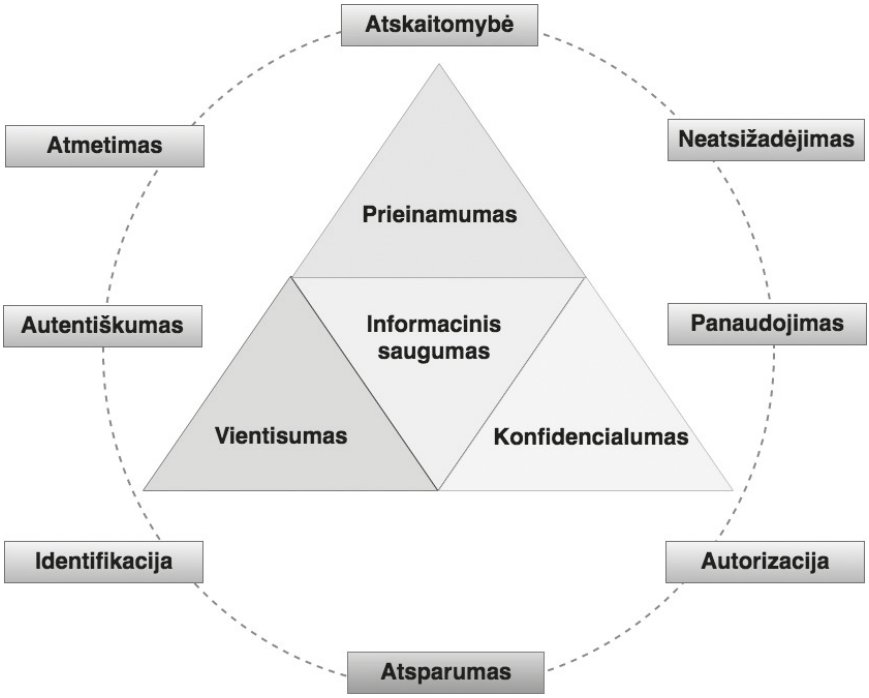
Kalbant apie literatūroje egzistuojančius informacinio saugumo apibrėžimus, kaip jau pažymėta šiame skyriuje, su kompiuterine sauga susijusioje literatūroje, įvairiose šios pramonės šakos ekspertų medijose bei akademiniuose domenuose pakankamai senai vyksta diskursas dėl vieningo informacijos saugumo termino nustatymo, tad skirtingi tyrėjai naudoja skirtingą terminiją. Zafar ir Clark (2009) pateikia vieną platesnių informacinio saugumo apibrėžimų. Pagal tyrėjus, informacijos saugumas suprantamas kaip „personalo mokymas informacijos valdymo ir bendrojo saugumo žinojimo srityje, potencialių grėsmių suvokimas, visų organizacijos valdymo sričių saugos politikų ir procedūrų formavimas, technologijų diegimas ir stebėsena bei nuolatinis jų vertinimas, informacijos saugos incidentų valdymo technikų integravimas“. Kiek siauresnis, tačiau išskiriantis konkrečius aspektus Galatenko (2006) pateiktas apibrėžimas, pagal kurį, informacinis saugumas suprantamas kaip „informacijos ir palaikomosios infrastruktūros apsauga nuo atsitiktinio arba sąmoningo natūralaus arba dirbtinio poveikio, kuris gali sąlygoti informacinius nuostolius informacinių santykių subjektams: palaikomosios informacijos infrastruktūros naudotojams ir savininkams“.

Literatūroje, pradedant ankstyvaisiais informacinės saugos teorinės minties laikotarpiais ir baigiant šių dienų tyrimais (Deswarte, Laurent, Blain, Fabre, 1991; Crosbie ir Spafford, 1995; Dhillon ir Backhouse, 2000; Diep ir kt., 2007; Chen ir Zhao, 2012; Uddin ir kt., 2015), dažnai sutinkamas informacijos užtikrinimo modelis, dar vadinamas, informacinio saugumo trikampiu ar informacinio saugumo triada, sudarytas iš trijų pagrindinių lygių, turinčių tam tikrą funkcinę paskirtį, užtikrinančių fundamentines informacijos apsaugos savybes: konfidencialumą, vientisumą, prieinamumą. Šiame modelyje esantys esminiai principai atspindimi ir egzistuojančiuose informacinio saugumo apibrėžimuose, pavyzdžiui JAV Nacionalinis standartų ir technologijų institutas apibrėžia informacinį saugumą kaip „informacijos ir informacinių sistemų apsaugą nuo neautorizuotos prieigos, naudojimo, atskleidimo, sutrikdymo, modifikavimo ar sunaikinimo, siekiant užtikrinti konfidencialumą, vientisumą ir prieinamumą“ (NIST, 2013). Elektroninės informacijos sauga yra įvardinama kaip „elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas“ (Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 2013).

Kaip akcentuoja Melnikov ir kt. (2008), informacijos konfidencialumas yra vienas svarbiausių integralaus saugumo aspektų, nepriklausomai kokiame lygmenyje būtų taikomas: nacionaliniame, konkrečios pramonės šakos plotmėje, organizaciniame ar individualiame. Pažymėtina, kad literatūroje ir praktikoje iš tiesų daug dėmesio skiriama organizacijų konfidencialumo aspektui. Tai gali būti paaiškinama tuo, kad tai yra ganėtinai svarbus aspektas valdymo, organizacijų komercinių, karinių ir valstybės paslapčių apsaugos domenuose,

taip pat jis turi didžiulę svarbą ir privačių duomenų apsaugos srityje. Pažymėtina, kad šie trys kertiniai informacinės saugos principai, daugelio ryškų indėlį informacinio saugumo srityje padariusių tyrėjų nuomone, negali būti nagrinėjami atskirai, o bent vieno jų atmetimas, gali sąlygoti informacinės saugos užtikrinimo proceso tęstinumo praradimą (Leiwo ir kt., 1999; Rosenthal, 2002; Byrnes ir Proctor, 2002; Nozaki ir Tipton, 2007; Ma, Johnston, Pearson, 2008), o tai gali būti ypač juntama dideles sistemas valdančiose ir specialių apsaugos priemonių joms reikalaujančiose organizacijose. Vėliau plėtodami informacinio saugumo teorines idėjas, kai kurie tyrėjai pabrėžė, kad informacinis saugumas yra daugiau nei tik bandymas pasiekti duomenų konfidencialumą, integralumą ir prieinamumą ir pasiūlė įtraukti atskaitomybės, panaudojimo, autorizacijos ir identifikacijos (Nozaki ir Tipton 2002) bei neatsižadėjimo (angl. non denial) aspektus. Neatsižadėjimas informacinės saugos kontekste turėtų identifikuoti, kad tam tikra informacinė žinutė buvo išsiųsta vienos šį faktą patvirtinančios šalies ir gauta kitos, kuri taip pat pritaria įvykusiam faktui (Byrnes ir Proctor 2002), kas yra ypač aktualu elektroninių dokumentų patvirtinimo bei pasirašymo laikais. Rao ir Nayak (2014) manymu, informacijos saugos priemonės taip pat apima ir informacijos autentiškumą ir netinkamos informacijos atmetimą (angl. *denial*). Kalbant apie valstybinių informacinių sistemų saugumą, pagal Zissis ir Lekkas (2011), e. valdžios domene vientisumo, konfidencialumo bei prieinamumo komponentai praplečiami papildomais dviem: autentiškumu, kuris šiame kontekste reiškia transakcijų ir komunikacijos metu bei dokumentacijoje naudojamų duomenų teisėtumą, ir atskaitomybe, kuri sąlygoja visų e. valdžios sistemoms grėsmę keliančių veiksnių atsekamumą bei už juos atsakingų šalių identifikavimą. Galiausiai, Singer ir Friedman (2013) pasiūlė **prie trijų egzistuojančių bazinių informacinio saugumo komponentų pridėti dar vieną papildomą – atsparumą**.

Apibendrinant anksčiau išdėstytus teiginius, galima suformuluoti konceptualų modelį, kurio centre yra informacinio saugumo trikampį sudarantys elementai, kurie papildomi kitų devynių, skirtingų autorių įvardintais kibernetinio saugumo elementais. Šie elementai, priklausomai nuo sistemos, gali būti formuojami tiek visi kartu, tiek pritaikant tik jų dalį. Autoriaus nuomone, be trijų kertinių informacinio saugumo komponentų, atsparumas yra būtinas kiekvienos sistemos elementas.



Šaltinis: *parengta autoriaus pagal Byrnes ir Proctor (2002); Tipton Nozaki (2007); Rao ir Nayak (2014); Zissis ir Lekkas (2011); Singer ir Friedman (2013).*

2 pav. *Papildytas informacinio saugumo trikampis*

Apibendrinant šį poskyrį, vertėtų pastebėti, kad egzistuojantis terminų sąmyšis yra dar labiau padidinamas bendro sutarimo dėl to, ką turėtų saugumas padėti pasiekti ir, kada galima sakyti, jog tai jau yra pasiekta nebuvimo, o kalbant tradiciniais vadybos terminais – valdymui vykdyti turi būti išmatuotinas objektas. Neabejotinai egzistuoja neformalus bendrasis suvokimas, kad saugumas turėtų apimti rizikas, kylančias informaciniams resursams, tačiau toks požiūris yra pakankamai siauras ir sudėtingai pamatuojamas, o pastaruoju metu vykstant skirtingas geopolitines stovyklas atstovaujančių valstybių informacinei priešpriešai bei masiškai klaidingos ar žalingos bei neteisėtos informacijos sklaidai (angl. fake news), akivaizdu, kad informacinio saugumo sąvoka turėtų būti praplečiama iki tam tikros informacinės visuomenės gyvybinėje erdvėje esančios informacinės erdvės apsaugos bei skaitmeninės ir kultūrinės šių visuomenių gerovės puoselėjimo.

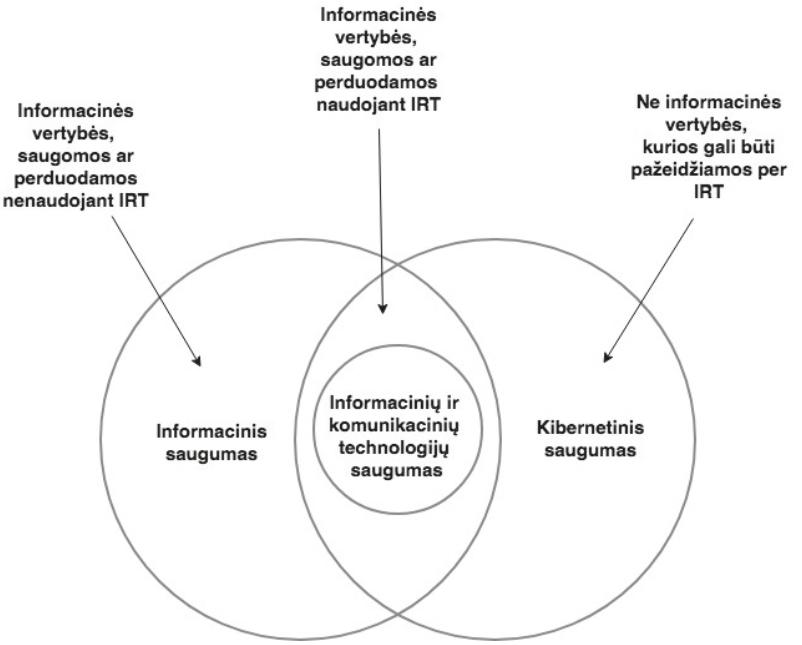
1.2. Informacinio saugumo konceptų plėtotė kibernetinio saugumo elementais

Kaip ir informacinis saugumas, kibernetinis saugumas turi aibę skirtingų apibrėžimų. Ilgą laiką kompiuterijos tinklų sauga buvo išskirtinai apibrėžto rato techninių ekspertų klausimu; šiuolaikiniam išplėstame saugumo kontekste valstybinio sektoriaus bei korporacijų

atstovai ir netgi individualūs asmenys yra neabejotinai priskiriami suinteresuotosioms šalims, kaip bendrosios kibernetinės saugos erdvės veikėjai. Tad kiekvieno joje dalyvaujančio subjekto saugumas gali būti suvokiamas skirtingai. Pagal Camp ir Lewis (2005), kibernetinis saugumas apima techninius, socialinius ir ekonominius aspektus ir, kadangi iš esmės jis pats yra moralinė vertybė (Nissenbaum, 2005), saugumo konceptas taip pat turi ir etinių savybių (Siponen, 2000). Saugumas turėtų būti vartojamas kartu su tokiomis sąvokomis kaip privatumas, intelektinės vertybės, lygybė, tačiau iki šiol jis buvo laikomas, visų pirma, technologine problema, nepaisant to, kad jis yra turtingas, kompleksiškas konceptas, sudarytas iš kintančių specializuotų ir bendrinių reikšmių (Nissenbaum, 2005).

Nemažai ekspertų taip pat diskutuoja dėl kibernetinio saugumo ir informacijos saugumo terminų tarpusavio pozicionavimo ir vartosenos. Dalis šių sričių atstovų mano, kad nepaisant to, jog kibernetinis saugumas yra informacinio saugumo dalis, kadangi kibernetiniame domene vykstantys reiškiniai neatsiejami nuo informacijos ir informacinių sistemų, šie terminai gali būti laikomi identiškais ir gali būti naudojami sinonimiškai arba keičiami priklausomai nuo konteksto[4]. Kiti ekspertai mano, kad kibernetinis saugumas yra naujasis informacinio saugumo evoliucijos etapas, jų nuomone, tai yra dvi tos pačios saugumo monetos pusės, tik kibernetinis saugumas pakelia tradicinį saugumo suvokimą į naują lygmenį, nes šis domenas neapsiriboja vien tik informacijos apsauga, o apima ir infrastruktūros apsaugos elementus. Todėl, praplėtus organizacijos informacinių resursų sąvoką kibernetiniu saugumu, organizacijos, nuosekliai vykdžiusios informacinio saugumo politiką neturėtų pajusti didelio neigiamo poveikio dėl šių sąvokų kaitos. Papildomu argumentu šiam požiūriui paremti galėtų būti ir faktas, kad ir iki tam tikro laiko neegzistavusiam kibernetinio saugumo terminui, infrastruktūrai, kaip informacijos valdymo sistemai, iš saugumo perspektyvų buvo skiriamas pakankamas dėmesys. Kai kurie ekspertai net mano, kad kibernetinio saugumo programas, įgyvendinamas organizacijų IRT departamentų, galima vykdyti paraleliai su informacinio saugumo programomis, už kurių plėtojimą būtų atsakingi organizacijų Informacinės saugos departamentai. Nepaisant nedidelio šių dviejų programų diferencijavimo, pagrindinis jų abiejų tikslas yra organizacijos vertybių saugos užtikrinimas. Atsižvelgiant į šį faktą, yra kritiškai svarbu, kad plėtojant organizacijos bendrą saugos strategiją jos būtų glaudžiai koordinuojamos (Rodrigues, 2014). Akademinėje bendruomenėje, kaip ir saugumo industrijoje, galima rasti įžvalgų dėl esminių kibernetinio ir informacinio saugumo skirtumų. Tyrėjai, kaip ir saugumo ekspertai-praktikai, pastebi, kad kibernetinio saugumo ir informacinio saugumo konceptai dažnai naudojami kaip sinonimai, tačiau nepaisant to, kad jų veiklos sritys, vertinant bendrame organizacijos informacinių vertybių saugos kontekste, iš esmės persidengia, šie du reiškiniai nėra visiškai identiški. Šiuos teiginius gerai iliustruoja Solms ir Niekerk (2013), kurie pažymi, kad kibernetinis saugumas ir jo priemonių pagalba vykdomas elektroninės erdvės kontroliavimas, apjungdamas savyje informacinį ir IRT saugumą (žr. 3 pav.), apsaugo ne informacinės prigimties vertybes, kurioms kyla grėsmė dėl IRT naudojimo.

4 https://www.novainfosec.com/2014/05/05/cyber-security-versus-information-security/



Šaltinis: *Solms ir Niekerk (2013)*
3 pav. *Informacinio, IRT ir kibernetinio saugumo sąsajos*

Pagal šį požiūrį, kibernetinis saugumas praplečia ir papildo informacinį saugumą.

1.3. Kibernetinės erdvės ir joje kylančių grėsmių aktualizavimas

Kibernetinės erdvės konceptualizavimas. Nuolat didėjantis kompiuterių skaičius ir ryšio tinklų technologijomis teikiamų sprendimų plėtra, naujų verslo modelių ir elektronine komunikacija paremtų socialinių technologijų atsiradimas sąlygojo naujos informacinės - kibernetinės erdvės susiformavimą, kuri atsirado XXI a. pradžioje, kai ant esamo kompiuterijos pagrindo buvo suformuotas visą jį apimantis naujasis konceptualus klodas. Liu ir kt. (2011) pažymi, kad informacija, perduodama iš kibernetinės erdvės, sąveikauja su fizinėmis ir mentalinėmis realaus pasaulio erdvėmis, o dirbtiniai sistemų aspektai – su realaus pasaulio aspektais. Kibernetinės–fizinės – socialinės sistemos vykdo savisinchronizaciją ir daro įtaką fiziniams, informaciniams, kognityviniams ir socialiniams domenams. Kibernetinė erdvė apjungia IRT tinklus, duomenų bazes ir informacijos resursus į globalią virtualią sistemą, kuri be informacinių technologijų paprasčiausiai negalėtų egzistuoti (Ben-Israel ir Tabansky, 2011). Kibernetinės erdvės struktūros apima ekonomiką, politiką, ginkluotąsias pajėgas, psichologiją ir informaciją (Grobler ir kt., 2011), socialinį ir infrastruktūrinį domenus (Lehto, 2013). Pagal tokį modelį, politinės struktūros yra atsakingos už nacionalinį

saugumą ir atviros visuomenės gyvybingumą, kariuomenė – už nacionalinio saugumo palaikymą ir visuomenės apsaugą nuo kibernetinio karo grėsmių. Vertinant psichologinių operacijų potencialą, ypač svarbi šioje aibėje yra psichologinė dimensija, kuri vaidina svarbų vaidmenį kibernetinėje erdvėje (Lehto, 2013). Kibernetinė erdvė yra daugiau nei internetas, tai nėra tik aparatinė ar programinė įranga, duomenys bei informacinės sistemos. Ji apima ir žmones, socialines sąveikas, vykstančias šiame tinkle ir infrastruktūroje (Lehto, 2013). Pagal Ben-Israel ir Tabansky (2011), kibernetinė erdvė apjungė egzistavusius informacinio saugumo sprendimus su naujomis priemonėmis bei sąlygojo atsirasti visą šią susiformavusią erdvę apimančius naujus kontrolės ir apsaugos mechanizmus – kibernetinį saugumą.

Kibernetinėje erdvėje kylančių grėsmių dinamika informacinių ir ryšio technologijų plėtros kontekste. Kibernetinio saugumo idėjų ir jo įgyvendinimo požiūrių plėtros nagrinėjimas būtų nepilnas neskiriant tinkamo dėmesio grėsmės konceptui. Šio poskyrio tikslas – apibrėžti kibernetinio saugumo grėsmes informacinių technologijų plėtros kontekste ir taip pabandyti atskleisti vis didėjantį grėsmių informaciniam saugumui mastą bei augantį jų sudėtingumo lygį. Informacinės technologijos yra būtent tas komponentas, kurio pagrindu formuojamos informacinio saugumo ir jo valdymo sistemos. Atsižvelgiant į tai, šiame poskyryje, technologijų plėtros ir jų skvarbos analizės kontekste nubrėžiant sąsajas tarp šių reiškinių plėtros nagrinėjamas informacinio saugumo vystymasis – nuo bandymų apsaugoti nedideles įtinklintas kompiuterines sistemas iki nacionalinės svarbos kritinės infrastruktūros apsaugos priemonių formavimo.

Tradicinio nusikalstamo išpuolio ar gamtinės katastrofos atveju grėsmė yra akivaizdi, ji turi pavidalą, dažniausiai galima nustatyti, ar šiuo metu ji aktuali, ar jau praėjusi. Kalbant apie kibernetinio saugumo grėsmes, pažymėtina, kad elektroninėje erdvėje saugos objektus atakuojantys šaltiniai charakterizuotini kaip neturintys aiškaus pavidalo, užslėpti, nežinia kada galintys pasireikšti, jų geografinė lokacija sunkiai nustatoma, ji gali būti netikra. Pagal Rao ir Nayak (2014) pasiūlytą terminiją, **grėsmė** kyla tuomet, kai atsiranda potenciali galimybė tam tikru būdu pažeisti informacinį saugumą. Bandymas realizuoti grėsmę apibūdinamas kaip **ataka**. Realizuojantysis ataką yra apibūdinamas kaip **piktavalis**, o potencialūs piktavaliai yra apibūdinami kaip **grėsmės šaltinis**. Grėsmė informacinio saugumo kontekste reiškia bet kokį reiškinį, keliantį pavojų informacijai, kompiuterijos resursams, vartotojams ar duomenims. Jos gali būti klasifikuojamos įvairiais būdais, tačiau esminis dalykas, kad jos pagal savo veikimą gali būti **vidinės** – kylančios organizacijos viduje, ir **išorinės** – organizaciją veikiančios iš už jos ribų, dažniausiai kylančios iš aplinkos, kurioje organizacija veikia (Rao ir Nayak, 2014). Kai kurios grėsmės paveikia visą organizaciją, kitos – tik jos dalis. Pagal jų rūšį, prie visų išvardintų apsaugos krypčių (tinklo, fizinės), gali būti skiriamos ir socioekonominės grėsmės, kurios gali būti specifinės ir aktualios konkrečiame regioniniame kontekste, taip pat teisinės grėsmės, socialinės inžinerijos grėsmės, kurios yra ypač pavojingos, nes jei piktavaliams pavyksta gauti prieigą prie riboto naudojimo resursų, šiems resursams iškyla tiesioginė grėsmė (Rao ir Nayak, 2014; Melnikov ir kt., 2008).

Sudėtinga būtų nesutikti, kad IRT ilgainiui tapo vienos pagrindinių moderniosios visuomenės varančiųjų jėgų, turėjusios ne ką mažesnę įtaką žmonijai nei kognityvinė,

agrokultūrinė ar industrinė revoliucijos. IRT sisteminė integracija įvairiose privataus ir viešojo sektoriaus vertikalėse sąlygoja reikšmingus šią sistemą tobulinančius veiksnius, tokius kaip greitis, kaštų mažinimas bei lankstumas. Didėjant institucijų priklausymo nuo technologijų mastui, auga ir kartu su technologijų naudojimu atsirandančių grėsmių sąrašas, o valdžios aparatas tampa pažeidžiamu tiek, kiek yra pažeidžiamos jo naudojamos technologijos (Liang, Xue, 2009). Informacinės technologijos yra tarsi „lazda turinti du galus“: kai yra naudojamos pagal paskirtį, jos turi milžinišką potencialą, galintį pagerinti žmonių ir organizacijų našumą, tačiau naudojamos netinkamiems tikslams, jos gali kelti didžiulius pavojus individams, organizacijoms ir visuomenei (Liang ir Xue, 2009), o tai dar labiau padidina joms kylančių rizikų tinkamo įvertinimo poreikį. Naujųjų technologijų plėtra ne tik keičia organizacijų veiklos modelius, bet ir sukelia grėsmę jų kasdienei veiklai. Tai apima visas žemiau išvardintas technologijas ir kanalus: internetas ir žiniatinklis, mobilūs įrenginiai, internetinė televizija, daiktų internetas (Sherwood, Clark, Leenas, 2005).

Siekiant geriau suvokti paraleles tarp IRT plėtros ir grėsmių informaciniam saugumui, vertėtų pasitelkti Andersen (2006) modelį, kuriuo nagrinėdamas IRT plėtros fazes, autorius šį procesą skirsto į keturis pagrindinius etapus. Pats pirmasis yra **Kultivavimas** (angl. *cultivation*), prasidėjęs 1970-aisiais ir trukęs iki ankstyvųjų 1980-ųjų. Jam būdingas specializuotų, sudėtingų kompiuterijos technologijų ekspertų ir inžinierių valdomų sistemų diegimas, veikiančių mainframe tipo kompiuterių ir nuotolinių, izoliuotų terminalų bei centralizuotų sprendimų pagalba. Kalbant apie saugumo būklę šiame konkrečiame IRT vystymosi etape, pažymėtina, kad nepaisant to, jog pasirodė pirmieji įsibrovimai į telekomunikacines sistemas (angl. *prhreaking*), dėl uždarų, vien vidiniams vartotojams prieinamų sistemų specifikos šis periodas laikytinas saugiausiu, nes pirminiai informacinės saugos taikymo poreikiai buvo sąlygoti būtinybės apsaugoti konkrečius apibrėžtoje vietoje esančius Mainframe kompiuterius. Tam pakakdavo gana paprastų priemonių, siekiant apsaugoti juos ir juose saugomą informacija nuo vagystės ar sugadinimo; jų fizinė sauga ir prieigos kontrolė buvo užtikrinamos vykdant žmogiškųjų resursų pagrindu suformuotą fizinę apsaugą, taikant fizines identifikacijos priemones. Taip iki interneto atsiradimo buvo išskirtinai taikoma tik fizinė duomenų apsauga (Rao ir Nyak, 2014). Antrasis etapas – **Sklaida** (angl. *seeding*) – prasidėjo IRT plėtrai įgavus pagreitį, kuris dėl savo galimybių automatizuotai atlikti masines užduotis sąlygojo naujų viešojo sektoriaus valdymo formų atsiradimą (Contini ir Lanzara, 2008), nulėmusį ir naujų informacijos valdymo technikų konceptualizavimo poreikį. Šis poreikis ypač tapo juntamas praėjusio amžiaus paskutiniais dviem dešimtmečiais (1980-aisiais ir 1990-aisiais), vykstant ryškiems inovacijų poslinkiams technologijų srityje bei palaipsniui vykstančiam didelių kompiuterijos terminalų keitimui asmeniniais kompiuteriais, kuris sąlygojo naujos grupės IRT vartotojų, neturinčių ekspertinių IRT žinių, atsiradimą. Tai lėmė situaciją, kai keletą gerai apmokytų viešojo sektoriaus IRT sistemų operatorių pakeitė aibė informacijos sistemų vartotojų, neturinčių tinkamų informacijos ir jos saugumo valdymo žinių ir įgūdžių. Atsirandant pirmiesiems asmeniniams kompiuteriams, paskirstytai kompiuterijai (angl. *distributed computing*) bei naujiems elektroninės informacijos apsikeitimo būdams, susiformavo ir pirmieji modernūs kibernetinio nusikalstamumo įrankiai. Atsirado pirmieji virusai Apple kompiuteriams. Xerox, Parc bendrovėse buvo sukurti pirmieji kompiuterių pažeidžiamumą išnaudojantys

„kirminai“ (angl. *worms*[5]), kurie nekontroliuojamai išplito tinklu ir pakenkė kelioms to meto sistemoms. Kiek vėliau, 1983 metais[6], buvo suformuota kompiuterinio viruso sąvoka. Šiuo laikotarpiu buvo vykdomi pirmieji sulaikymai Didžiojoje Britanijoje dėl neteisėto įsilaužimo į karališkosios šeimos narių pašto dėžutes[7].

Dėl to, Didžiojoje Britanijoje buvo pradėti pirmieji kibernetinius nusikaltimus reglamentuojančių teisės aktų kūrimo žingsniai, 1990 m. išleistas „Netinkamo kompiuterių naudojimo aktas“[8] . Trečiąjį etapą Andersen (2006) įvardina **Išplitimu** (angl. *extension*). Šis etapas, vykęs pradedant nuo 1990-ųjų vidurio ir trukęs iki ankstyvųjų 2000-ųjų, turėjo ypač stiprų poveikį informacinio saugumo konceptualiai kaitai. Iki šiame etape vykusio interneto atsiradimo ir ankstesniame etape įvykusio asmeninių kompiuterių masinio išplitimo, kompiuterių operavimo procesai vyko silose, o su interneto atsiradimu įvykusi technologijų valdymo decentralizacijos viešajame sektoriuje pradžia sąlygojo suvokimą, kad informacinių technologijų valdymo klausimai turi būti integruoti į pagrindines valdžios funkcijas (Yildiz, 2007), o jų sauga įtraukta į bendrąją viešojo sektoriaus technologijų organizavimo ir valdymo darbotvarkę. Interneto pirmtako Arpanet[9] tinklo plėtros pradžioje, kai tik ribotas skaičius vartotojų jį naudojo skirtingose lokacijose ir sistemose esančių duomenų perdavimui, informacijos sauga nebuvo kritiškai svarbus dalykas, tačiau, laikui bėgant, prie tinklo jungiantis vis daugiau vartotojų bei į jį patenkant vis daugiau duomenų, informacinės saugos poreikis ėmė sparčiai augti (Rao ir Nyak, 2014). Šiame etape plėtojantis interneto TCP/IP[10] protokolų pagalba veikiančioms technologijoms pradėtos vykdyti pirmosios standartinės transakcijos bei standartizuotos paslaugos. Šiam laikotarpiui būdinga naujo modelio informacinio saugumo nusikaltimų banga – sukurtas „Kaos“[11] virusas, o užkrėstas programinis kodas išplito daugybėje kompiuterių. Įvyko pirmieji įsibrovimai į valstybinius tinklalapius: programišiai pakeitė JAV teisingumo departamento, CŽV ir JAV karinių oro pajėgų svetainių turinį[12], kiek vėliau buvo „nulaužtas“ JAV Baltųjų rūmų tinklalapis. Prieš kelis valstybinius, karinius ir universitetų tinklalapius JAV surengtos DDoS[13] atakos. Surengti išpuoliai prieš The New York Times tinklalapį. Išleistas pirmasis „Trojan“[14] tipo virusas, suteikiantis prieigą prie užkrėstų kompiuterių. Sukurtas „Melissa“[15] virusas, apkrečiantis tekstinius dokumentus ir pašto programos kontaktų sąrašus, DDoS atakomis nulaužti Yahoo, Amazon, eBay, CNN[16] ir kt. komerciniai tinklalapiai. Atrastas pirmasis

5 https://www.techopedia.com/definition/4171/worm

6 http://csrc.nist.gov/publications/nistir/threats/subsubsection3_3_1_1.html

7 http://itsecurity.co.uk/2015/03/hacking-the-royal-male-the-computer-misuse-act/

8 http://www.legislation.gov.uk/ukpga/1990/18/contents

9 http://www.darpa.mil/about-us/timeline/arpanet

10 http://www.tcpipguide.com/

11 http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=4046

12 http://www.sptimes.com/Hackers/history.hacking.html

13 Ataka naudojanti daugybę kompiuterių (angl. *Denial of Service*) (NIST, 2013).

14 https://usa.kaspersky.com/internet-security-center/threats/trojans#.V96eGJN96Rs

15 https://www.sans.org/security-resources/idfaq/what-was-the-melissa-virus-and-what-can-we-learn-from-it/5/3

16 https://www.cnet.com/news/leading-web-sites-under-attack/

virusas „Palm“[17] sistemos nešiojamiems delniniams kompiuteriams. Microsoft pranešė apie tai, kad į jų vidinį tinklą buvo įsilaužta ir užpuolikai priėjo prie konfidencialaus bendrovės programinio kodo[18]. Daugybėje bendrovės Microsoft produktų aptiktos saugumo spragos. Programišiai įsilaužė į Kalifornijos valstijos vyriausybinę svetainę bandydami pasiekti informaciją apie valstybės tarnautojus. JAV valdžia išleido perspėjimą, kad Kinijos valstybės remiami Kinijos programišiai gali pradėti atakas visoje JAV (Symantec, 2006). Tokiame kontekste IRT plėtra pasiekė ketvirtąjį savo lygmenį, Andersen (2006) įvardintą **Įsiskverbimu** (angl. *penetration*). Šiam laikotarpiui, prasidėjusiam 2000-ųjų viduryje, būdinga visur esanti interneto prieiga, kuri sąlygoja sistemos savininkiškumo perkėlimą išoriniams vartotojams. Ji realizuojama mobiliosios kompiuterijos ir belaidės prieigos pagalba. Ėmus diegti šias technologijas automobiliuose, buitinėje įrangoje, taikant išmaniųjų pastatų sprendimus, ėmė formuotis daiktų interneto sąvoka. Atsiradus naujiems technologiniams sprendimams, gimė ir nauji kibernetinio nusikalstamumo būdai: naudojant bevielę prieigą įvykdyti įsilaužimai į automobilines sistemas[19], kitus įtinklintus objektus[20], 2016 m. spalio mėnesį pasinaudoję saugumo spragomis, programišiai įvykdė didžiulio masto ataką prieš DNS[21]paslaugą teikiančios bendrovės infrastruktūrą, taip sutrikdydami aibę masiškai lankomų interneto tinklalapių (Twitter, Spotify, PayPal, Verizon, Playstation ir kt.) veiklą. Verta pažymėti, kad atakai buvo panaudoti įvairūs tinkle esantys neapsaugoti įrenginiai, tokie kaip saugos kameros, interneto maršrutizatoriai ir pan.[22] Pažymėtina, kad nagrinėjant Andersen (2006) IRT plėtros fazes, stebima aiški technologijų evoliucija nuo uždaro vidinio vartojimo (angl. *in house*) modelio link prasiskverbimo už organizacijos ribų, perkeliant sistemų savininko vaidmenį išoriniams vartotojams. Kuo sistema yra labiau išplečiama už organizacijos ribų, tuo sunkiau užtikrinti jos saugumą, nustatyti už saugumą atsakingus asmenis, deleguoti jiems konkrečias saugumo užtikrinimo užduotis. Plėtojantis technologijoms organizaciniame lygmenyje, atsiranda įvairūs faktoriai, niveliuojantys organizacines ribas, taigi susiformuoja įdomus paradoksas – **technologijos, kurias reikėtų apsaugoti nuo kibernetinių grėsmių, kuo labiau yra plėtojamos, tuo didesnes prielaidas sudaro šioms grėsmėms atsirasti.** Be technologijų plėtros tam tikrą poveikį jų saugumui turi ir jų decentralizacija. Kalbant apie viešojo sektoriaus technologijas, pažymėtina, jog egzistuoja nuomonė, kad intranetinių sprendimų atsisakymas galėtų būti vienu iš strateginio mąstymo krypčių plėtojant IRT viešajame sektoriuje, o tai būtų dar didesnis poslinkis nuo informacinio siloso koncepto. Šis fenomenas valdžios institucijų dažnai suvokiamas kaip decentralizuojanti tendencija, vedanti prie biurokratinės kontrolės praradimo bei administracinės netvarkos sklidimo. Siekdama užkirsti kelią netvarkai valdžia stengiasi įgyvendinti griežtesnę kontrolę bei normatyvinį reguliavimą, kuris visada turi kontraversišką efektą ir yra sunkiai pamatuojamas (Contini ir Lanzara, 2008). Šiuo atveju, intranetas simbolizuoja

17 http://www.computerworld.com/article/2588338/mobile-wireless/first-palm-virus-found--but-risk-to-users-said-to-be-low.html

18 https://www.theguardian.com/world/2000/oct/27/qanda.markoliver

19 http://fortune.com/2016/01/26/security-experts-hack-cars/

20 https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/

21 http://www.webopedia.com/TERM/D/DNS.html

22 https://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/

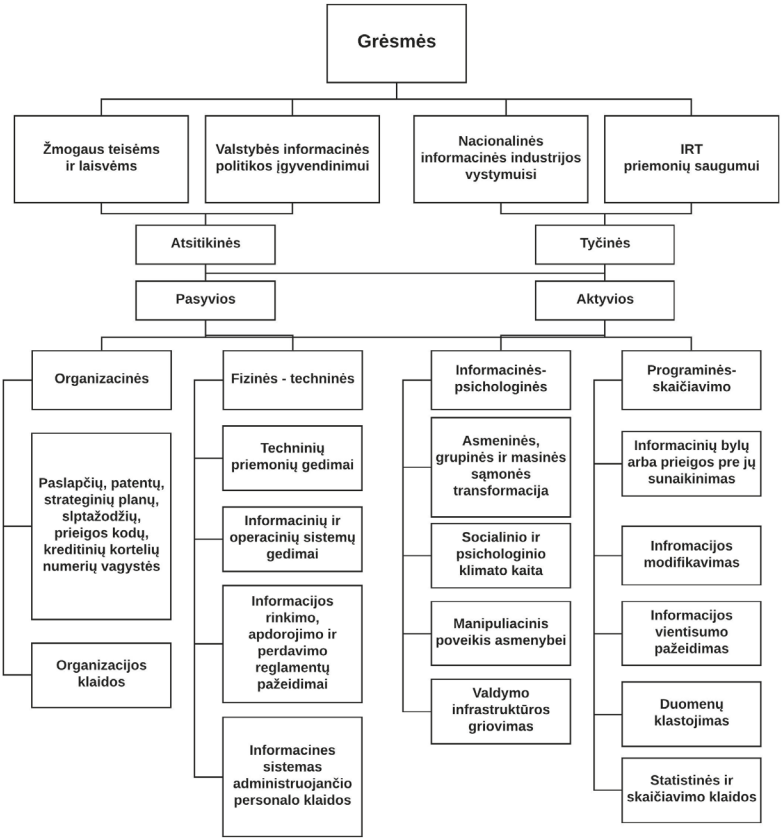
valdžios sistemų uždarumą ir tokios kontrolės įgyvendinimą arba raudonąją juostą, kuri atskiria viešojo sektoriaus sistemas nuo likusio pasaulio (Welsh ir Pandey, 2006). Tai padeda užtikrinti geresnį sistemų saugumo lygį, tačiau koncentruojant per didelį dėmesį į intranetinio siloso palaikymą, išnaudojami didesni energijos kiekiai siekiant nustatyti kontrolės ribas nei teikiant paslaugas, veiklų orientacija yra išimtinai nukreipiama į vidines rutinas, kurios retai kada būna skaidriomis ar įtraukia išorinius elektroninių paslaugų vartotojus (Andersen, 2006). Kaip rodo esama praktika, IRT paplitimas dažnai implikuoja technologijų atitolimą nuo intensyviai reguliuojamos organizacinės ir institucinės terpės (Nardi ir Kallinikos, 2007). Organizacinių valdymo technologijų naudojimas dažnai būna pagrįstas koncentracijos modeliu, savo ruožtu, IRT yra matomos kaip palaikančios mastelių kaitą ir dispersiją (Kallinikos, 2009). Organizacijos formoms kintant į labiau tinklines, atsiranda nuotolinių (įtinklintų) kompiuterinių darbo vietų formavimo ir už organizacijos ribų saugomų informacinių vertybių naudojimo galimybės, asmeninės kompiuterinės įrangos naudojimo darbo vietose BYOD fenomenas[23] . Visi šie procesai didina galimų saugumo grėsmių skaičių ir kelia papildomus iššūkius bendros organizacijos informacinio saugumo sistemos vientisumui. Modernios IRT aplinkos, fiziniams reiškiniams suteikdamos tam tikro neapčiuopiamumo bei įgalindamos informacijos sklaidą, jos buvimą visose įmanomose laikmenose, tinkle, organizacijos intranete, ir taip lemdamos tam tikrą jos saugumo svarbos suvokimo infliaciją, sąlygoja tai, kad organizacijų veikėjams yra sudėtinga informaciją prilyginti vertybei ir ją tokia suvokti.

Kibernetinės erdvės grėsmių transformacija. Didėjant pačios kibernetinės erdvės skverbties mastui atsiranda ir naujos grėsmių formos, gerokai praplečiančios tradicines, informacinio saugumo kontekste suvokiamas grėsmes, nagrinėtas ankstesniame poskyryje. Ant egzistuojančių programinės įrangos pažeidžiamumų ir neteisėtos prieigos, tarsi papildomas sluoksnis, prisideda tokios grėsmės kaip kibernetinis šnipinėjimas, kibernetinis karas ir kitos nelegalios veiklos kibernetinėje erdvėje bei naujos kibernetinės priešpriešos formos.

Pakankamai plačią grėsmių klasifikaciją pateikia Melnikov ir kt. (2008). Autorių modelyje grėsmės pagal jų poveikio vektorių skirstomos į keturias kategorijas, t.y.:

- žmogaus teisėms ir laisvėms;
- valstybės informacinės politikos įgyvendinimui;
- nacionalinės industrijos vystymuisi;
- IRT priemonių saugumui.

23 https://www.ibm.com/mobile/bring-your-own-device/



Šaltinis: *Melnikov ir kt. (2008)*

4 pav. *Grėsmių klasifikacija*

Plėtojant kibernetinėje erdvėje kylančių grėsmių diskursą, vertėtų paminėti ir grėsmes, sąlygotas naudojant tinkle esančius kompiuterius, kaip terpę prieš sociumą nukreiptoms, griaunamoms struktūroms formuoti, vykdyti žalingą komunikaciją. Tai apima tinklalapius, skatinančius rasinę, etninę neapykantą, taip pat tuos, kuriuose koordinuojama, planuojama nusikalstama, sukčiavimo veikla, tinklalapiai ir kiti duomenų apsikeitimo mechanizmai, platinantys nepilnamečių pornografiją bei medijos, naudojamos organizuoti teroristinėms atakoms, jų planavimui bei su jomis susijusios informacijos apsikeitimui. Taip pat egzistuojant įvairioms hibridinės priešpriešos formoms, vis dažniau internetas yra naudojamas kaip propagandos ir prieš konkrečias valstybes nukreiptos informacijos skleidimo terpė. Taip pat vertėtų pažymėti ir grėsmes kritinei socialinei infrastruktūrai, komunalinėms paslaugoms, priklausomoms nuo interneto, bankinėms, valdžios, švietimo, sveikatos apsaugos sistemoms, komercinėms ir komunikacijų medijoms. Kritinės sistemos yra vis labiau priklausomos nuo įtinklintų informacinių sistemų ir yra pažeidžiamos tinklu vykdomų atakų

(Nissenbaum, 2005). Vis dažniau vienos valstybės tinkle esanti infrastruktūra tampa kitos – priešiškos valstybės kibernetinių atakų taikiniu. Kalbant apie kibernetines grėsmes sukeliančių objektų motyvaciją, vertėtų prisiminti Lehto (2013) suformuotą kibernetinių grėsmių motyvacinių faktorių modelį, paremtą kelių autorių darbais. Pagal Lehto (2013) egzistuoja penkios pagrindinės, žmogaus motyvaciniais faktoriais pagrįstos kibernetinių grėsmių kategorijos. Šie motyvaciniai faktoriai yra: egoizmas, anarchija, pinigai, destrukcija ir galia (Cavelty, 2010; Ashenden, 2011; Lehto, 2013).

Nagrinėjant kibernetines grėsmes pagal vykdomas veiklas ir jas vykdančius subjektus, literatūroje skirtini penki pagrindiniai lygmenys:

- Pirmasis lygmuo – kibernetinis aktyvizmas. Apimantis kibernetinį vandalizmą, įsilaužimą ir haktyvizmą (angl. *hacktivism*)[24]. Ryškiausi atstovai yra Anonnymous grupuotė[25]. Pagal Ayala (2016), haktyvizmas – ardomasis kompiuterių ir kompiuterinių tinklų naudojimas, siekiant skleisti tam tikras politines idėjas.
- Antrasis lygmuo – kibernetinis nusikalstamumas. Jis apima nusikaltimus, atliekamus naudojant elektronines priemones, komunikacijų tinklus, informacines sistemas arba veiksmus, nukreiptus prieš šias sistemas ir tinklus (Commission of the European Communities, 2007).
- Trečiasis lygmuo – kibernetinis šnipinėjimas. Veiksmai atliekami tinkle, kompiuterinėse sistemose, nukreipti neteisėtais veiksmais gauti slaptą, jautrią, nuosavybinę, įslaptintą informaciją iš individų, konkurentų, specifinių grupių, valdžios, siekiant politinės, karinės ar ekonominės naudos. Pagal Ayala (2016), kibernetinis šnipinėjimas – yra aktas arba praktika, kai bandoma gauti slaptus duomenis (asmeninius, jautrius, komercinius arba įslaptintus) be informacijos savininko leidimo. Kibernetinis šnipinėjimas dažnai naudojamas vienų šalių prieš kitas, siekiant kitų šalių ekonominių iniciatyvų pagalba pagerinti savo pačių ekonominį gerbūvį ir padidinti proveržį mokslo ir inovacijų srityje (Ben-Israel ir Tabansky, 2011). Cituojant Mowbray (2013): „Kibernetinis šnipinėjimas pastaraisiais laikais yra pasiekęs epidemijos lygmenis, paveikiančius tiek pažangiausias pasaulio bendroves, tiek valstybines institucijas. Žala apima terabaitus prarastos intelektinės informacijos bei pasisavintų finansinių vertybių".
- Ketvirtasis lygmuo – kibernetinis terorizmas, vykdomas naudojantis tinklais, nukreiptas prieš kritinę infrastruktūrą ir jos kontrolės ir valdymo priemones. Šių atakų tikslas yra pridaryti žalą, bei sukelti baimę visuomenėje bei padaryti spaudimą atakuojamos šalies politiniams lyderiams. Pagal Ayala (2016), kibernetinis terorizmas suvokiamas kaip kompiuterinio tinklo naudojimas, siekiant nutraukti kritinės nacionalinės infrastruktūros veiklą arba terorizuoti ir bauginti valdžią ar piliečius. Galutinis kibernetinio terorizmo rezultatas – pažeisti kritinę infrastruktūrą bei kibernetinėje erdvėje esančias ir jos tarpusavyje siejamas kontrolės struktūras.
- Penktasis lygmuo – kibernetinis karas, jis sudarytas iš trijų atskirų elementų: strateginio kibernetinio karo, taktinio - operacinio kibernetinio karo ir žemo intensyvumo konfliktų. Saugumo studijų diskurse kibernetinis domenas laikomas penk-

24 Žodis atsiradęs apjungiant žodžius hakeris ir aktyvizmas

25 https://en.wikipedia.org/wiki/Anonymous_(group)

tuoju karo domenu, po žemės, jūros, oro ir kosmoso (Ayala, 2016). Kibernetiniams karams visiškai negalioja karų taisykles apibrėžiančiose tarptautinėse konvencijose nustatyti karinių konfliktų, fizinės konfrontacijos, teritorinių atakų ir kiti principai (Ben-Israel ir Tabansky 2011). Kibernetinio karo suvokimo gyliui įgyti reikėtų suvokti keletą skirtingų šį reiškinį sudarančių aspektų:

- kompiuterinis karas – kompiuteriai, šiuo atveju, atlieka pagrindinės informacijos laikymo ir transportavimo priemonės vaidmenį;
- elektroninis karas – šiuo atveju, kiekviena oponuojanti pusė priešpriešą nukreipia į kitos pusės sensorines ir komunikacijos priemones;
- psichologinis karas – apima medijų naudojimą, kariuomenės ir žiniasklaidos konvergenciją, manipuliavimą informacija (Ben-Israel ir Tabansky 2011).

Kaip pažymi Lehto (2013), nėra vieningo kibernetinio karo apibrėžimo – dažniausiai šis terminas naudojamas apibrėžti valstybinių veikėjų kibernetinėje erdvėje vykdomas operacijas, todėl dažnai jis suvokiamas kaip karinių operacijų dalis. Gilinant kibernetinio saugumo grėsmės suvokimą, vertėtų išskirti Cavelty (2014) suformuotas keturias kategorijas, kuriose pagal taikymo sritis ir jose dalyvaujančius tipinius veikėjus, tipinius objektus ir grėsmes pateikiami kiekvienai informacinio saugumo kategorijai būdingi aspektai, pateikiami 1 lentelėje.

1 lentelė. Saugumo kategorijos

	I. Techninė	II. Nusikaltimų – šnipinėjimo	III. Valstybinės saugos	IV. Karinė
Tipiniai objektai	Kompiuterija	Privatus sektorius	Kritinė informacijos infrastruktūra	Kibernetinės ginkluotosios pajėgos
	Kompiuteriniai tinklai	Viešasis sektorius	Visuomeninės funkcijos kibernetinėje erdvėje	Nacija / valstybė
Veikėjai	Programišių subkultūra Kompiuterinės saugos ekspertai Antivirusų pramonė	Verslo sektoriaus atstovai Antivirusų pramonė Teisėsauga Žvalgybos bendruomenė	Nacionaliniai saugumo ekspertai Kibernetinė sauga / nacionalinė sauga	Nacionaliniai saugumo ekspertai Kariuomenė
Grėsmės	Kenkėjiškos programos Tinklų griovimas Įsilaužimas į sistemas Visos kitos nelegalios veiklos	Specializuotos kenkėjiškos programos Kibernetnis nusikalstamumas Valstybinis kibernetinis šnipinėjimas	Kritinės infrastruktūros sutrikdymas Kibernetinis terorizmas Priešiškų valstybių kibernetiniai padaliniai	Katastrofinės atakos prieš kritinę infrastruktūrą Kibernetinis terorizmas Kibernetinis šnipinėjimas Priešiškų valstybių kibernetiniai padaliniai

Šaltinis: *Cavelty (2014)*

Sudėtinga pasakyti, ar toliau besiplėtojant IRT sprendimams šios grėsmių klasifikacijos ir formos yra galutinės. Grįžtant prie Andersen (2006) pasiūlyto modelio baigiamosios įsiskverbimo fazės, vertėtų pastebėti, kad pats šios klasifikacijos autorius pažymi, jog augant technologijų kompleksiškumo lygiui, didėjant įvairių interakcijos modelių skaičiui, įsiskverbimo fazė, galbūt, nėra tiksliausias šių dienų IRT sistemų struktūros apibūdinimas. Be to, jis nėra tiksliausias atspirties taškas, padėsiantis parodyti, kaip atrodys organizacinės struktūros ateityje. Tačiau, jo nuomone, informacinių sistemų kaitos pokyčio taškas bus labiausiai susijęs su tolimesnėmis organizacinių ribų ryškumo mažėjimo tendencijomis – tai sąlygos tarporganizacinių ir vidinių organizacijos tinklų modelių ir standartų stiprėjimą (Andersen, 2006), lydimą dar didesnių iššūkių informacijos saugumo srityje.

1.4. Kibernetinio saugumo valdymo aktualizavimas

Kalbant apie informacinio saugumo valdymo specifiką, pažymėtina, kad ankstyvosiose saugumo plėtros stadijose šis konceptas nagrinėtas pakankamai siaurai ir, lyginant su kitais informacinio saugumo porūšiais, egzistuoja pakankamai mažas informacinio saugumo valdymo aspektus apimantis tyrimų skaičius (Hong ir kt., 2003). Kalbėdami apie informacinio saugumo valdymo pozicionavimą organizacijoje, Rao ir Nayak (2014) pažymi, kad jis dažniau matomas veikiau kaip nereikalinga blogybė, turinti mažai praktinės vertės, nei kaip veiklos procesus įgalinanti priemonė. Tai yra taikytina įvairiuose organizacijos lygmenyse, pradedant aukščiausioje valdymo grandyje, kai formuojant tradicinius informacijos saugumo modelius, procesas pradedamas nuo saugumo politikos apibrėžimo, kas yra laikoma sudėtingu ir daug laiko atimančiu uždaviniu, baigiant operacijų lygmenyje patiriamais iššūkiais. Informacinio saugumo valdymas įgaus didesnį palaikymą organizacijoje, jei ji bus diegiama atsižvelgiant į organizacijos veiklos tikslus bei reikalavimus. Informacinės technologijos įgalina informacinį saugumą, o tai galiausiai atsiperka, kai yra apsaugoma organizacijos veikla, jos paslaugų vartotojai, partneriai ir pačios sociotechinės infrastruktūros ir programos. Būtent dėl šių priežasčių būtina užtikrinti, kad veiklos, IT ir informacijos saugos strategijos būtų subalansuotos ir papildytų vienos kitas (Rao ir Nayak, 2014).

Istoriškai kibernetinio saugumo tyrimai susiduria su pakankamai sudėtinga situacija, kai būtina gauti su praktiniais tyrimų lauko aspektais susijusius duomenis, tačiau tai padaryti yra pakankamai sudėtinga dėl uždaros kibernetinio saugumo prigimties. Nepaisant to, kad visi veiksmai yra atliekami kibernetinėje erdvėje, taikant kompiuterines priemones, tai tampa ne vien tik kompiuterijos mokslų tyrimų objektu, o vykstant vis glaudesnei socialinių ir technologinių sistemų konvergencijai, kibernetinio saugumo klausimų nagrinėjimui iš tarpdisciplininės perspektyvos turėtų būti skiriamas vis didesnis dėmesys (Ben-Israel, Tabansky 2011). Kibernetinio saugumo domene pastebimas technologinių tyrimų dominavimas arba, kaip įvardina Dhillon ir Backhouse (2001), mechanistinė orientacija, kuri turėjo didžiulę įtaką informacinių sistemų plėtrai organizacijose. Mechanistinių modelių koncentracija yra tiesiogiai nukreipta į technologijų ekonominius, fizinius ir informacijos apdorojimo aspektus. Toks požiūris ignoruoja sudėtingų socialinių veiksnių, kuriuose vyksta technologijų plėtra kontekstą, o užstrigę ties mechanistiniu požiūriu į organizacijas,

dauguma informacinių sistemų profesionalų nepaiso sociopolitinių informacinių sistemų aspektų, kas neišvengiamai sąlygoja nelankstumo ir nesėkmės efektus (Kling, 1980).

Kalbėdami apie informacinio saugumo valdymą iš sisteminės perspektyvos, Eloff ir Eloff (2003) pažymi, kad informacinio saugumo valdymas suvokiamas kaip valdymo sistema, skirta suformuoti ir išlaikyti saugią informacinę aplinką, ir jis turi būti vykdomas diegiant procesus bei procedūras, skirtas informacinių technologijų saugumui valdyti. Pagal Rao ir Nayak (2014), saugumo valdymas yra kelias skirtingas valdymo kryptis apimantis procesas, kurį sudaro šie procesai:

- Informacijos apsaugos lygio būtinybės nustatymo įvertinimas ir atitinkamų užduočių formavimas.
- Organizacijos informacinės saugos būklės duomenų surinkimas ir analizė, rizikų informacijai įvertinimas.
- Priemonių rizikų apdorojimui planavimas; atitinkamų kontrolės mechanizmų realizavimas ir diegimas.
- Rolių ir atsakomybių paskirstymas.
- Personalo mokymai.
- Operatyvinės informacijos saugos užtikrinimas.
- Kontrolės mechanizmų funkcionavimo stebėsena, jų efektyvumo vertinimas ir atitinkamų koreguojančių veiksmų vykdymas.

Kibernetinio saugumo domene, kaip ir kitose įvairiose technologijų taikymo srityse, požiūris į IRT kito nuo perdėtai optimistiško, technologijas matančio sidabrine kulka, galinčia išspręsti visas problemas, iki visiško nusivylimo IRT, sąlygoto didžiulių, neefektyvių investicijų į technologijas, neskiriant dėmesio efektyviam jų panaudojimui. Ankstyvuoju savo gyvavimo laikotarpiu kibernetinis saugumas buvo laikoma išskirtinai techninės srities ekspertizės reikalaujančia sritimi, kurioje didžiausias dėmesys skiriamas būtent technologiniams dalyko aspektams. Tačiau ilgainiui technokratinis požiūris pasirodė neefektyvus, tapo aišku, kad sėkmingas IRT ir informacinių sistemų diegimas nebūtinai garantuoja sėkmingą valdžios saugumo sistemų transformaciją (Tseng ir kt., 2008), todėl mokslo bendruomenėje bei privačiame sektoriuje vis labiau ėmė stiprėti nuomonė, kad kibernetinis saugumas turi būti nagrinėjamas platesniame – holistiniame kontekste, integruojančiame žmogiškąjį faktorių, IRT valdymo principus, procesus ir našumo rodiklius į vienalytę operacinę visumą, kurioje ypač svarbus vaidmuo turi būti skiriamas ir vadybinei dedamajai (Singh ir kt., 2013; 2012; Phillips, 2013; Siponen, ir kt., 2014; Soomro ir kt., 2014). Dėmesio koncentracija aukščiausiame lygmenyje turi pasislinkti nuo vien tik į IRT strategijų plėtojimą koncentruotą link tokio, kuris apimtų strateginius ir politinius bei institucinių valdymo inovacijų elementus (Tseng ir kt., 2008), nes, kaip rodo pakankamai ilga technologijų taikymo patirtis, nepakanka vien įdiegti technologijų ir nepagrįstai tikėtis norimo optimistinio rezultato – būtina įgyvendinti ir organizacinius pokyčius, kurie dažnai ir yra sudėtingiausias organizacinės kaitos aspektas. Organizacinio ir individualaus inertiškumo sąlygojami IRT plėtros viešajame sektoriuje trukdžiai pakankamai plačiai aprašinėjami e. valdžios literatūroje, nuo pat jos ištakų, kaip vieni esminių, e. valdžios progresą trukdančių veiksnių (Layne ir Lee, 2001). Egzistuojanti teisinė aplinka ir esami valdymo būdai sąlygoja, kad viešojo sektoriaus institucijoms yra žymiai sunkiau įgyvendinti pokyčius nei privataus, o

didžiosios finansinės organizacijos gali dar jautriau reaguoti nei valstybinės į bet kokius su vadybos procesu susijusius pasikeitimus (Soomro ir kt., 2016). Šios tendencijos aktualios tiek iš organizacijos valdymo, tiek iš joje dirbančiųjų darbuotojų perspektyvos, pavyzdžiui, Stanton ir kt. (2005) nagrinėdami galutinio vartotojo saugumo perspektyvas pastebėjo, kad tam tikra, su saugumu susijusi elgsena skirtingose pramonės srityse ir veiklos sektoriuose yra skirtinga, o vartotojo elgsenos ypatumai pasižymi tuo, kad organizacijose, ypač priklausomose nuo informacinės saugos užtikrinimo, galutiniai paslaugų vartotojai daug atsakingiau vertina informacinės saugos kontrolės reikalavimus. Taip vertinant statistinę organizaciją, kurios veikla visiškai nepriklauso arba mažai priklauso nuo informacinės saugos valdymo, galima daryti išvadą, kad tokioje organizacijoje nebus ir deramos kibernetinės saugos valdymo struktūros.

Kibernetinio saugumo valdymas pakankamai neseniai susiformavusi, bet nuolatos evoliucionuojanti tyrimų sritis, IRT sistemų taikymu praplėtusi ilgą laiką egzistavusį valdymo organizacijų našumo, produktyvumo ir žmogiškųjų resursų valdymo teorijų lauką. Nors pats informacinio saugumo konceptas yra ganėtinai senas ir pradėjo plėtotis su pirmaisiais žmonių informacijos perdavimo būdais bei bandymais apsaugoti jautrią komercinę ar valstybinės svarbos informaciją, dabartinis elektroninės informacijos saugos suvokimas tapo įmanomas tik įvykus telekomunikacijų technologijų proveržiui, atsiradus interneto pagrindu veikiančioms technologijoms ir jomis teikiamoms paslaugoms. Saugumo valdymo konceptų evoliuciją puikiai iliustruoja Von Solms ir Von Solms (2005) bei Kim (2007) idėjos, teigiančios, kad konceptas, kurį kažkada buvo galima vadinti tiesiog duomenų sauga, vėliau tapo kompiuterių sauga. Šis reiškinys vėliau išsivystė į IRT saugą, laikui bėgant, IRT sauga tapo informacijos sauga, kurią, didėjant įtinklintų procesų mastui ir augant rizikų, kylančių dėl netinkamos organizacijos elektroninių resursų apsaugos skaičiui, vėliau išplėtė virsmas į verslo bei veiklos saugumą. Viską vainikavo kibernetinis saugumas, kai dėl globalizacijos, blunkančių organizacijų ir valstybių ribų kyla būtinybė apsaugoti ne tik atskiras organizacijas, pavienes informacijos formas ar veiklos procesus, bet ir visą komunikacijų ir veiklos (kibernetinę) erdvę (Von Solms ir Von Solms, 2005). Taigi, IRT technologijos ir su naujais valdymo modeliais atsiradusios ir masiškai išplitusios elektroninės informacijos mastai bei naujas požiūris į grėsmes sąlygojo kokybiškai naujų kibernetinio saugumo valdymo technikų atsiradimo poreikį. Kaip rodo praktika, realiomis sąlygomis ateities saugumas labiau priklausys nuo gebėjimo peržiūrėti senas idėjas ir pakeisti egzistuojančius procesus, o tai padėtų susidoroti su didesne rizikų aibe per kuo trumpesnį laiką.

Kibernetinio saugumo valdysena. Besiplėtojant kibernetinio saugumo valdymo teorijoms, ilgainiui šiame tyrimų lauke pradėta taikyti valdysenos koncepcija. Apie ją kalbėdami Solms ir Solms (2009) pažymi, kad informacinio saugumo valdysena apima valdymo grandies įsipareigojimus ir lyderystę, organizacinių struktūrų formavimą, vartotojų žinojimą ir įsipareigojimus, politikas, procedūras, procesus, technologijas ir atitikties užtikrinimo mechanizmus. Siekiant užtikrinti organizacijos elektroninių vertybių konfidencialumą, vientisumą ir prieinamumą, būtina įgyvendinti tęstinį šių anksčiau išvardintų faktorių plėtojimą. Kalbėdami apie informacinio saugumo valdymo ir valdysenos skirtumus Solms ir Solms (2009) pažymi, kad informacinės saugos valdymas yra saugumo valdysenos dalis, tad valdymas vyksta bendrame valdysenos procese kaip sub-procesas. Bandant tai suvokti

iš procesų hierarchijos perspektyvos, informacinės saugos valdysena prasideda pačiame viršuje ir apima visus organizacijos darbuotojus, kurie yra bendrojo organizacijos informacinės saugos valdysenos modelio dalis. Informacinio saugumo valdymas yra labiau apčiuopiamas procesas, užtikrinantis, kad būtų suformuotos ir įdiegtos saugos politikos ir procedūros bei užtikrintas sklandus kasdienių saugos operacijų užduočių vykdymas (Solms ir Solms, 2009). Moulton ir Coles (2003) apibrėžia informacinio saugumo valdyseną kaip „kontrolės aplinkos suformavimą ir palaikymą, siekiant suvaldyti rizikas, susijusias su informacijos konfidencialumu, vientisumu ir prieinamumu". Pagal autorius, tai apima ir palaikomuosius procesus ir sistemas, užtikrinančias tinkamai suformuotus ir įdiegtus valdysenos mechanizmus, taip pat kasdienes administracines veiklas – saugumo operacijas – bei naujų, su IRT sprendimais arba procesais susijusių saugumo sistemos konstrukcinių elementų plėtrą.

Pagal klasikinį suvokimą, valdysena apibūdinama kaip visų valdymo procesų aibė, įgyvendinama konkrečioje plotmėje – konkrečioje geografinėje teritorijoje, formalioje ar neformalioje organizacijoje ir materializuojama įstatymų, normų ar žodinės galios pagalba. Iš valdysenoje dalyvaujančių veikėjų perspektyvos valdysena apima visų šių veikėjų tarpusavio interakcijas, sprendimų priėmimus, kolektyvinius problemų sprendimus, sąlygojančius socialinių normų ir institutų sukūrimą, jų stiprinimą bei plėtrą (Hufty, 2011). Kalbant apie IRT valdyseną, kuri yra informacinio saugumo valdysenos pagrindas, pažymėtina, kad egzistuoja aibė šio reiškinio pavadinimų. JAV IT valdysenos institutas (angl. *IT Governance Institute*) teigia, kad IRT valdysena yra lyderystė, organizacinės struktūros ir procesai, kurie užtikrina, kad organizacijos IRT palaiko ir praplečia organizacijos strategijas ir tikslus (IT Governance Institute, 2001).

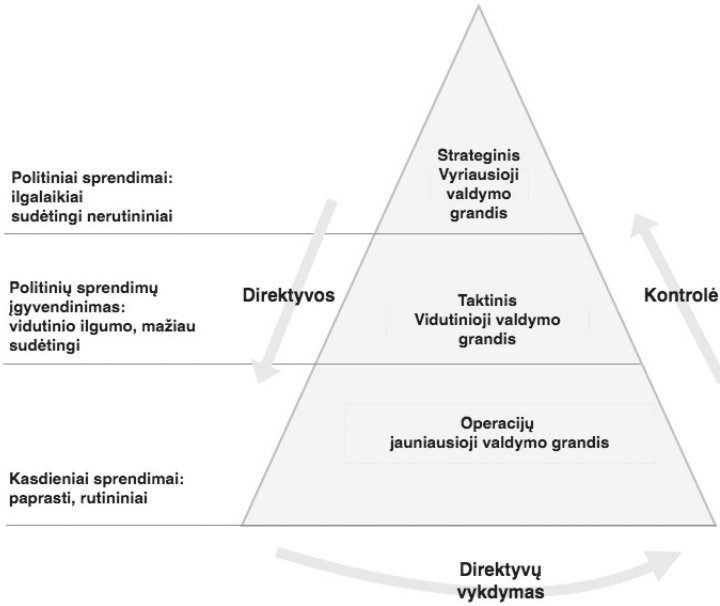
Atsižvelgiant į IRT integralų vaidmenį šiuolaikinėje organizacijoje ir į tai, kad, plačiąja prasme, kibernetinės saugos valdysena yra bendrųjų organizacijos valdymo krypčių dalis ir, visų pirma, yra ne techninis, o valdymo ir veiklos organizavimo aspektas, saugumas turi būti kritiniu modernios organizacijos planavimo ir valdymo komponentu (Chang ir Ho, 2006), o tam būtina identifikuoti priemones, kurių pagalba būtų užtikrinamas tinkamas valdymo uždavinių organizavimas. Šiam tikslui įgyvendinti, svarbu tinkamai suvokti kibernetinės saugos valdymo kontekstą. Kibernetinės saugos valdysena yra keleto veiklos sričių sankirtoje esantis konstruktas, apjungiantis vadybinius – informacinių technologijų, korporacijų valdysenos bei išskirtinai techninius informacinės saugos klausimus. Vertėtų pažymėti, kad kibernetinio saugumo valdysenos specifikos kaita nevyko izoliuotai, vakuume, ji kito kartu su kitomis organizacijos valdysenos sritimis. Augantis pavojų informacijai kiekis skatina informacinį saugumą integruoti į organizacijos bendruosius valdymo modelius ir suteikti šiai sričiai aukščiausios svarbos statusą kartu su kitomis kritiškai svarbiomis sritimis (Fazlida ir Said, 2015). Atsižvelgiant į tai, literatūroje dažnai skiriama aibė kibernetinio saugumo dimensijų, padedančių suvokti nagrinėjamą dalyką iš skirtingų perspektyvų bei integruoti jos logines dalis su kitais veiklos organizavimo klausimais. Literatūroje vis plačiau kalbama apie kintančias atsakomybės tendencijas ir vykstantį atsakomybės už saugumo plėtrą poslinkį nuo techninę ekspertizę turinčių organizacijos profesionalų link organizacijos vadybinės grandies (Soomro ir kt., 2016). Valdymo svarba informacinės saugos domene akcentuojama įvairius saugos aspektus nagrinėjančių autorių. Chang ir Ho

(2006) bei Philips (2013) atkreipia dėmesį, kad organizacijoje turi būti suformuota saugumo valdymo struktūra bei taikomos apibrėžtos valdymo praktikos, kurios daro itin didelę įtaką bet kokių IRT sistemų efektyvumui.

Baigiant šio poskyrio diskusiją būtina akcentuoti, kad nepriklausomai nuo valdymo veiksmams apibūdinti vartojamos terminijos (valdymas ar valdysena) bei valdymo objektų suvokimo kaitos (informacinis saugumas, kibernetinis saugumas), skaitmeninės ekonomikos laikais tinkamas informacinio saugumo užtikrinimas yra tiesiogiai priklausomas nuo tinkamų šalies valstybinių organizacijų informacinių resursų saugumo valdymo veiksmų, kitaip tariant, bendrasis valstybės informacijos saugumo valdymas prasideda infrastruktūros lygmenyje ir vis dažniau tęsiasi į nacionalinio saugumo dalį elektroninėje erdvėje, kur jo konceptuali suvoktis yra praplečiamas nuo technologinių sistemų iki sociopolitinių institutų ribų. Tačiau labai svarbu suvokti, kad informacinio saugumo valdymas organizacijose nėra vien tik su IRT susijęs klausimas. Ypač svarbi ir žmogiškoji informacinio saugumo faktoriaus dedamoji.

1.4.1. Kibernetinio saugumo valdymo lygiai organizacijoje: strateginis, taktinis, operacijų

Nagrinėjant kibernetinio saugumo sistemos vadybinį konstruktą, pažymėtina, kad jis yra sudarytas iš skirtingų vadybinių dedamųjų, apimančių skirtingus valdymo požiūrius bei užtikrinančius vadybos užduočių įgyvendinimą skirtinguose organizacijos valdymo lygmenyse. Vienas būdų nagrinėti šiuos lygius yra taikyti trijų lygmenų valdymo sprendimų priėmimo modelį, pagal kurį, vadybos uždaviniai sąveikauja su informacinės saugos struktūriniais elementais skirtinguose organizacijos sprendimų priėmimo lygmenyse: strateginiame, taktiniame, operacijų. Solms ir Solms (2005) savo modelyje pripažįsta, kad informacinio saugumo valdysena yra integrali bendrosios organizacijos valdymo sistemos dalis, tad informacinio saugumo modelyje turėtų būti numatytos bendrosios organizacijos ir informacinio saugumo valdysenos sistemų sąsajos. Solms ir Solms (2005) suformuotas saugos valdysenos modelis išskiria du pagrindinius principus: tyrėjų nuomone, saugos valdysena turi apimti visus organizacijos valdymo lygmenis, t.y. strateginį, taktinį ir operacijų, taip įtraukiamos visos organizacijos veiklos procesus vykdančios sritys nuo valdymo grandžių vertikalės viršaus link jos apačios. Antrasis esminis principas yra tas, kad būtina išskirti tris atskiras veiklas, būdingas visiems anksčiau minėtiems lygmenims, t.y. nukreipimas, vykdymas ir kontrolė. Būtent šių veiklų numatymo faktas, Solms ir Solms manymu, sąlygoja tai, kad modelis gali būti suvokiamas būtent kaip valdysenos, o ne tiesiog kaip valdymo.



Šaltinis: *Von Solms ir Von Solms (2009); BBC Bitesize (2014)*
5 pav. *Kibernetinio saugumo valdymo lygmenys*

Strateginis lygmuo. Strateginiame lygmenyje yra valdysenos komponentai apimantys politines organizacijos dimensijas, ilgalaikius, kompleksiškus aukščiausios vadybinės grandies priimamus sprendimus, įtakojančius bendrines organizacijos plėtos kryptis. Jame kuriama saugos valdysenos politika, kuriai didžiulę teigiamą įtaką turi ne tik organizacijos kibernetinės saugos specialistų, bet ir aukščiausios grandies vadovų dalyvavimas (Kwon ir kt. 2012), formuojami bendriniai personalo valdymo principai, nustatomi saugių operacijų principai (Whiteman, Mattord, 2012), įvertinamos rizikos ir pavojai, šiame lygmenyje užduodamas pagrindinis klausimas: **„Kodėl?“**. Saugumo perspektyvoje, pagal White (2009), šis klausimas užduodamas atsakyti, kodėl egzistuoja organizacijos saugos problemos. Tai klausimas, už kurio slypi visa organizacijos kibernetinės saugos valdymo organizavimo esmė, kurios pagalba formuojamos saugos politikos, vertinamos išorinės ir vidinės grėsmės bei atsakoma į su žmogiškais faktoriais susijusius iššūkius. **Politikos** – sudaro pagrindą, užtikrinantį, kad sistemos yra formuojamos bei operuojamos laikantis saugumo reikalavimų, įvertinant vidines ir išorines rizikas ir grėsmes. **Vidinių ir išorinių grėsmių ir rizikų vertinimas** – proaktyvus ir dinamiškas, technologijų kaitą įvertinantis požiūris, bandant nustatyti potencialius pavojus. Grėsmių ir rizikų prioretizavimas, saugos biudžeto formavimas. **Žmogiški faktoriai** – poslinkio nuo technologijų vykdymas, suinteresuotųjų šalių (angl. *stakeholders*) poreikių tenkinimas. Suinteresuotosios šalies sąvoka verslo organizacijos kontekste apima reguliavimą vykdančias valdžios institucijas, akcininkus, klientus, darbuotojus

ir verslo partnerius. Valstybinės organizacijos kontekste papildomai reikia atsižvelgti į teisės aktus, etinius principus, elgesio kodeksus bei visuomenės poreikius. Taip priskiriant Von Solms ir Von Solms (2009) kibernetinės saugos dimensijų požiūrio kontekste išskiriamą korporatyvinio valdymo dimensiją, kuri sudaro pagrindą visoms kitoms organizacijos valdymo praktikoms, suformuoja jų veiklos procesams atskaitos tašką. Tyrėjų manymu, kibernetinės saugos valdyseną būtų sudėtinga nagrinėti atskyrus nuo organizacijos korporatyvinio valdymo konteksto. Korporatyvinis valdymas suvokiamas kaip mechanizmų, procesų ir sąsajų, politikų, standartų, procedūrų ir kitų teisės aktų visuma, kurios pagalba, korporacijos yra kontroliuojamos ir nukreipiamos konkrečia kryptimi (Shailer, 2004). Korporatyvinis valdymas apibrėžia ir vykdo stebėseną bei įvertina, ar rezultatai atitinka nustatytus planus; jis yra pagrindinis mechanizmas, kuris padeda organizacijoje veikiančioms suinteresuotoms šalims suderinti savo veiksmus siekiant organizacijos tikslų (Von Solms, Von Solms, 2009). Atsižvelgiant į tai, kad jis yra sudarytas iš aukščiausios grandies vadovų, valdybos direktorių bei kitų suinteresuotų šalių, korporatyvinis valdymas yra vieną didžiausią įtaką turinčių valdymo sričių. Informacinės saugos korporatyvinio valdymo kontekste aukščiausios grandies vadybininkų dalyvavimas yra kritiškai svarbus tęstiniam saugos valdysenos veiklų tobulinimui (Ezingeard, Bowen-Schrire, 2007), efektyvių programų formavimui (Knapp ir kt. 2006). Jis yra būtent ta organizacijos sistemos dalis, kurioje vyksta organizacijos, kokia ji bebūtų – valstybinė ar privati, veiklos krypčių ir organizacijos kontrolės mechanizmų nustatymas (Von Solms, Von Solms, 2009). Korporatyvinis valdymas apima procesus, per kuriuos nustatomi ir siekiami korporacijų tikslai, socialiniame, reguliavimo ir aplinkos kontekste (OECD, 2004). Korporatyvinis valdymas yra kaip skėtis, po kuriuo telpa organizacijos personalo, finansinių ir materialiųjų išteklių bei IRT valdymas, taip pat jį galima būtų suvokti kaip konteinerį, kuriame sutelpa visos kitos organizacijos informacinės saugos dimensijos (Von Solms, Von Solms, 2009). Atskirai vertėtų pažymėti, kad korporatyvaus valdymo grandies dėmesys informacinės saugos valdymo srityje turėtų pasislinkti nuo sukoncentruoto išskirtinai vien tik į IRT, sauga turėtų būti bendra-organizacinis dalykas. Taip pat būtinas bendras informacijos vertės suvokimas (Mitchell, Marcella, Baxter, 1999), kuri yra vienas vertingiausių organizacijos resursų (Von Solms, Von Solms, 2009). Toks suvokimas, kartu su dalies atsakomybės už informacijos saugą perkėlimu organizacijos valdybai, padėtų ieškoti sąlyčio taškų tarp organizacijos bendrojo valdymo ir kibernetinės saugos valdymo iniciatyvų. Strateginio lygmens privalumas yra konkurencinis pranašumas, valdančiųjų grandžių informuotumas apie esamas problemas, grįžtamas ryšys apie rizikas, galinčias paveikti stakeholderius, deramo patikrinimo lygio užtikrinimas, kaštų mažinimas, pasitikėjimo tarp organizacijos ir jos partnerių didinimas, pelno didinimas (Birchall ir kt., 2004). Kalbėdami apie strateginį saugumo valdymo lygį, Solms ir Solms (2005) skiria jame vykstantį nukreipimo (angl. *direct*) reiškinį ir pažymi, kad šiame etape valdyba turėtų aiškiai identifikuoti, kiek yra svarbios organizacijos informacinės vertybės ir, kokį vaidmenį jos atlieka bendrame organizacijos strateginės vizijos formavimo procese bei pažymėti, kaip svarbu organizacijai yra saugoti šias vertybes.

Taktinis lygmuo. Nors iš veiklos organizavimo perspektyvos taktinis lygmuo, būdamas svarbia jungtimi tarp strateginio ir operacijų valdymo lygmenų, ko gero, kibernetinio saugumo literatūroje tai vienas mažiausiai išnagrinėtų lygmenų. Vienas iš nedaugelio autorių,

nagrinėjusių šį lygmenį, White (2009), pastebėjo, kad kibernetinio saugumo valdymo domene, taktinis lygmuo apima veiksmus, kurių metu formuojamos ir diegiamos saugos sistemos, tam, kad būtų įgyvendinami strateginiame lygmenyje politikos formavimo etape išskirti uždaviniai, jame atsakoma į klausimą: **„Kaip galėtų būti sušvelninamos saugos problemos?“**. Kaip pripažįstama bendrinėje vadybos literatūroje, taktinis lygmuo turi mažesnį sudėtingumo lygmenį nei strateginis. Jame vykdomos šios pagrindinės veiklos: planavimas, dizainas (projektavimas), standartų nustatymas bei saugos užduočių įgyvendinimas. Jame formuojamos užduotys darbuotojams, saugos veiksmų planai. Taip pat tai apima valdymo ir kontrolės priemonių, apibrėžtų saugos politikose įgyvendinimą, informacijos srautų tėkmės krypčių nustatymą bei informacinių vertybių apibrėžimą (Kim ir Leem, 2005; White, 2009; Whitman ir Mattord, 2012). Planavimas – apima incidentų valdymą identifikavimą ir reagavimą; ekstremalių situacijų valdymą, krizių valdymą ir veiklos atstatymo operacijas; veiklos tęstinumą – atsarginių sistemų ir darbo vietų planavimą, nenutrūkstamų operacijų vykdymą. Dizainas (projektavimas) – apima saugos perimetrų, kontrolės procedūrų formavimą (Kim ir Leem, 2005); techninius dizaino komponentus: ugniasienių ir jų filtrų, VPN tunelių diegimas, įsibrovimo identifikavimo sistemų formavimas (Whitman ir Mattord, 2005, p. 288). Standartų nustatymas – apima detalių saugos politikų palaikymo uždavinių nustatymą bei sistemų diegimo, valdymo ir operacijų reikalavimų nustatymą (Whitman ir Mattord, 2005; White, 2009). Diegimas (angl. *implementation*) – apima saugos kontrolės priemonių diegimą, taikant projektinio valdymo principus (White, 2009) bei kitas vadybines ir procedūrines praktikas. Taktinio lygmens sėkmingos veiklos rezultatas yra padidintas organizacijos pasitikėjimo savo pajėgumais ir atskaitomybės lygis. Užtikrinama atitiktis reguliavimo ir teisinių mechanizmų keliamiems reikalavimams. Sumažinama rizika ir padidinama kontrolė, pagerinama prieiga prie informacijos, gerėja santykis su organizacijos partneriais. Pagal Solms ir Solms (2005), į taktinį lygmenį iš valdybos patekusios direktyvos veikia kaip indėlis ir yra detalizuojamos informacinės saugos politikų, procedūrų bei organizacijos standartų pagalba. Šie vykdymo dokumentai pasitelkiami apibrėžti taktiniame lygmenyje vykdomų veiklos procesų išeigą ir atspindėti vidutinės grandies organizacijos vadybininkų požiūrį į informacijos apsaugos priemones (Solms ir Solms, 2005).

Operacijų lygmuo. Operacijų valdymas apima saugos politikų palaikymą ir stebėseną, jame atsakoma į klausimą: „**Ką? Ką daryti?“.** Arba, pagal White (2009), kokias saugos praktikas ir procedūras taikyti. Šiame lygmenyje naudojamos auditavimo, fizinės kontrolės priemonės, tinklo skenavimo ir tinklo paketų fiksavimo (angl. *packet sniffer*) įranga. Palaikymas – operacijų valdymas apima kasdienių kontrolės, prieigos metodų bei vartotojų valdymo funkcijų palaikymą. Tai apima prieigos kontrolę, slaptažodžių valdymą. Stebėsena – įsibrovimo aptikimo ir įsibrovimo prevencijos sistemos, žurnalinių bylų analizė, įsibrovėlių sekimas bei „masalų“ bei saugių zonų (angl. *honey pots*[26]*, padded cells*) jiems įrengimas, vartotojų stebėsena, pranešimų (angl. *alerts*) valdymas (White, 2009). Iš vadybinių sprendimų priėmimo perspektyvos laikytinas mažiausią sudėtingumo laipsnį turintis lygmuo. Tačiau kalbant apie operacijų svarbą kitiems lygiams, taikytina White (2009) saugos valdysenos informacijos sklaidos teorija, pagal kurią, taikant iš apačios į viršų einančią perspektyvą, operaciniame lygmenyje gauti transakcijų duomenys tarnauja indėliu

26 https://en.wikipedia.org/wiki/Honeypot_(computing)

į informacijos formavimą. Šios informacijos vientisumo, konfidencialumo ir prieinamumo palaikymas bei stebėsena yra pagrindinis tikslas, vykdant operacijas, visas šis procesas palaikomas organizacijoje taikomomis procedūromis ir gairėmis. Operacijų metu gauta informacija, patekusi į taktinį lygmenį, yra interpretuojama ir naudojama sprendimų priėmime. Tolimesnė informacijos analizė ir jos agregacija sukuria žinias, reikalingas priimti strateginio lygmens sprendimus. Pagal šį požiūrį, visi lygmenys yra pakankamai svarbūs vien dėl to, kad priklauso vienas nuo kito. Operacijų lygmens ypatumai – užtikrinamas veiklos tęstinumas, saugi ir patikima prieiga prie informacijos. Gerinamas paslaugų vartotojų aptarnavimas, sistemos apsaugomos nuo neautorizuotos prieigos (White, 2009). Svarbi operacijų lygmenyje vykdoma veikla yra valdymo grandies informuotumo užtikrinimas. Sąsajos tarp strateginio ir operacijų lygmens, užtikrinamos įgyvendinant operacijų žinomumo (angl. *operational awareness*) funkciją. Nagrinėjant informacinio saugumo riziką iš įvairių organizacinių perspektyvų, galima būtų išskirti kelis pagrindinius faktorius, kurie turi būti įvertinti organizacijose diegiant net pačius paprasčiausius informacinės saugos modelius. Visų pirma, tai vykdančiosios organizacijos valdžios informuotumas, tiksliau kalbant, dėl organizacijos nepakankamo ar netinkamo informuotumo laipsnio egzistuojantis pavojus, kad ji nesupras organizacijai kylančios rizikos masto. Kai nėra patikimų duomenų, vykdančiajai valdžiai gali iškilti problemų bandant įvertinti potencialias dabartines rizikas, su kuriomis ji susiduria konkrečiu metu bei gali susidurti ateityje. Pačių duomenų nebuvimas nėra vienintelė problema. Tačiau vertėtų suvokti, kad nepaisant to, jog galima įgyvendinti visišką vadybinį informuotumą, gali susiklostyti situacija, kai duomenų kiekis yra pakankamas, tačiau dėl statistinių operacinių rizikų duomenų analizės metodų nepakankamo išplėtojimo, susidaro kita didelė kliūtis įgyvendinant organizacijos informacinį saugumą – tinkamų operacijų rizikos analizės įrankių nebuvimas. Tai gali sąlygoti netinkamų sprendimų priėmimą (White, 2009).

1.4.2. Kibernetinio saugumo valdymo aktualizavimas nacionalinio saugumo kontekste

Kadangi kibernetinio saugumo reiškinys vis dažniau integruojamas į nacionalinio saugumo įgyvendinimo darbotvarkę, tradicinės, technokratinės informacinio saugumo teorijos pasiekia savo teorizavimo ribas. Norint jas praplėsti ir siekiant suvokti kibernetinio saugumo vaidmenį bendrame valstybės saugumo sistemos kontekste, būtina ieškoti naujų teorinių perspektyvų, kurias galima būtų įtraukti į egzistuojančius modelius. Vienas tokių potencialiai integruotinų elementų yra saugumo studijų srityje egzistuojantys požiūriai. Tokią būtinybę sąlygoja vis dažnėjantys kibernetiniai incidentai, keliantys grėsmę nacionaliniams valstybių interesams ar jų saugumui. Vieni pirmųjų ryškiausių tokio pobūdžio kibernetinio saugumo incidentų – JAV – Kinijos saugumo apžvalgos komisijos įvardintas kaip vienas didžiausių pavojų amerikietiškųjų technologijų saugumui buvo 2003 m. Kinijos programišių organizuota, gerai parengta kibernetinio šnipinėjimo serija, nukreipta prieš JAV gynybos sektoriaus organizacijas, pavadinta „Titaniniu lietumi“ (angl. *Titan rain*)[27] .

27 https://www.theguardian.com/technology/2007/sep/04/news.internet

Tarp kinų taikiniu tapusių, karinę ir kosminę įrangą gaminančių bei tyrimus šioje srityje atliekančių organizacijų buvo tokie gerai žinomi vardai kaip NASA ir Lockhead Martin. Pagrindinis šių atakų tikslas buvo pagrobti kuo daugiau naujų įslaptintų technologijų informacijos. Šis kibernetinio šnipinėjimo atvejis neabejotinai pareikalavo peržiūrėti egzistuojantį požiūrį į tinkle vykstančius nusikaltimus bei aukštesnio prioriteto suteikimą kibernetinio saugumo grėsmėms.

Pažymėtina, kad sąsajų tarp nacionalinio ir kibernetinio saugumo paieškos nėra naujas reiškinys. Šių idėjų pradžia galima būtų laikyti tarptautinių santykių Kopenhagos mokyklos saugumo studijų domene pradėtus bandymus apibrėžti kitokias nei karines grėsmes, kurių pastaraisiais laikais atsiranda vis daugiau, jų daromas poveikis konkrečios šalies valstybingumui gali būti pakankamai ryškus, tačiau jas ganėtinai sudėtinga teorizuoti remiantis egzistuojančiais saugumo modeliais. Visų istorinių karinių konfliktų metu kylanti konvencinė grėsmė buvo lengvai identifikuojama; tai konkretus pavojus, dažniausiai kylantis iš už suverenaus subjekto teritorinių ribų, kurio šaltinis – kitokias vertybines, politines pažiūras turintis, kitam ideologiniam blokui priklausantis subjektas. Tačiau, kaip rodo pastarųjų dešimtmečių įvykiai, grėsmės sąvoka vis labiau plečiasi ir, nors toldama nuo karinio prado, įgyja vis platesnes apimtis (Buzan, Wæver, Wilde, 1997). Kariniu požiūriu grėsmė gali būti apibrėžiama „kaip veiksmas arba įvykių seka, kuri kelia grėsmę per trumpą laiką sumažinti konkretaus teritorinio vieneto (valstybės) gyventojų gyvenimo kokybę; kelia grėsmę reikšmingai susiaurinti valstybės valdžios, nevyriausybinių ir privačių subjektų politinės valios raiškos ir priimamų sprendimų aibę“ (Ullman, 1983). Taigi, tokios grėsmės atveju, visų pirma reikėtų nustatyti jos lygį ir šaltinį. Kalbant apie lygį, dažnai tai yra pakankamai nesudėtinga padaryti, tačiau šaltinio nustatymas gali būti pakankamai sudėtingas, be to, šiuo atveju, negalioja priešo iš kito teritorinio vieneto suvokimas, nes grėsmės šaltinis gali būti vidinis. Šie teiginiai tampa ypač aktualūs mąstant apie kibernetinio konflikto kontekstą. Vertėtų pažymėti, kad didėjant įtinklintų paslaugų skaičiui bei socialinėms sistemos vis labiau integruojantis su technologinėmis, kibernetinių žalingų veiksmų įvykių seka elektroninėje erdvėje yra pakankamai reali grėsmė konkretaus geografinio vieneto gyventojų kokybei. Saugumo studijų krypties atstovai saugumą suvokia kaip tam tikrą visų bendrai įgytų vertybių apsaugos išraišką, kaip vertę, kurios valstybė gali turėti daugiau arba mažiau. Jų manymu, tauta yra saugi iki tol, kol jai nekyla grėsmė paaukoti savo pamatinių vertybių, o tai suformuoja pagrindą požiūriui, teigiančiam, kad saugumo lygis kyla su valstybės gebėjimu atgrasyti atakas arba jas atremti (Buzan, Wæver, Wilde, 1997). Taip pat atskirai vertėtų panagrinėti saugumo studijų domene taikomus teorinius požiūrius ir, kaip šiuos požiūrius atstovaujančios teorinės mokyklos suvokia kibernetinį saugumo keliamus iššūkius bendroje saugumo sistemoje. Šio poskyrio tikslas nėra išsami tarptautinių santykių teorijų analizė, o labiau bandymas nustatyti, kaip egzistuojančios atskiros tyrimo lauko teorijos galėtų būti integruojamos kibernetinio saugumo studijų kontekste, siekiant išspręsti kibernetinio saugumo iššūkius iš nacionalinio saugumo perspektyvų.

Realizmas. Iš keleto egzistuojančių tyrimų tradicijų tarptautinių santykių ir saugumo srityje, kaip pripažįstama saugumo studijas nagrinėjančioje literatūroje, didžiausią įtaką turėjo realistų atstovai. Egzistuoja keletas skirtingų realistinių požiūrių (klasikinis, neoklasikinis, gynybinis, puolamasis ir kt.) į saugumo studijas, tačiau visi šio teorinio lauko

įvairias pakraipas atstovaujančių tyrėjų tematika apima keletą pagrindinių teiginių: valstybės yra centriniai tarptautinės politikos veikėjai; tarptautinė tarptautinių santykių politika yra anarchiška; tarptautinės politinės sistemos veikėjai yra racionalūs, nes jų veiksmai maksimizuoja jų pačių interesą; visos valstybės trokšta galios, tokiu būdu bandydamos užsitikrinti savisaugą ir išlikimą (Goodin, 2010). Karai, pagal realistus, įvyksta dėl pernelyg agresyvių konkrečių valstybių politikų arba šalių vidinių politinių sistemų sudarančių prielaidas godžioms vietinėms grupėms vykdyti savanaudę, ekspancionistinę užsienio politiką, kuri pati dėl ją vykdančių blogų žmonių yra blogis (Spirtas 1996). Nemažą indėlį saugumo studijų srityje įnešė neorealistai, kurie šiek tiek kitaip matė konflikto priežastis, pavyzdžiui, vienas ryškiausių neorealistinių idėjų atstovų Kenneth Waltz jau ne taip akcentavo blogojo lyderio ir jo motyvacijos vaidmenį (Elman, 2008). Saugumo studijose nemažą vaidmenį suvaidino ir gynybinio neorealizmo idėjos. Gynybinis neorealizmas būdamas struktūrine teorija yra neorealizmo teorijos dalis. Neorealizmo (taip pat gynybinio realizmo) pradas formuojamas iš realizmo ir vadovaujasi aibe panašių prielaidų: tarptautinės sistemos yra anarchinės; valstybės iš prigimties turi tam tikras puolamąsias karines galias, kurios suteikia galimybę pažeisti ar net sunaikinti viena kitą; valstybės negali būti tikros dėl kitų valstybių intencijų; pagrindinis šalių motyvas yra išgyvenimas; šalys strategiškai mąsto apie tai kaip išgyventi tarptautinėje sistemoje (Mearsheimer, 1995). Ant gynybinio realizmo pagrindo suformuotas puolamasis realizmas papildė anksčiau išdėstytas prielaidas tezėmis, teigiančiomis, kad didžiosios galios yra pagrindiniai veikėjai pasaulinėje politikoje, vykdomoje anarchinėje tarptautinėje sistemoje. Kalbėdami apie internetą, kaip kibernetinių konfliktų ir kibernetinio saugumo terpę, neorealistai jį mato kaip anarchinę sistemą ir pripažįsta, kad kibernetinė erdvė tapo naujuoju tarptautiniu mūšio lauku (Adams 2001), kurios nekontroliuoja jokia valdžios struktūra ar policinė jėga, kur jokiems kariniams ar ekonominiams blokams nepriklausančios valstybės yra atsakingos kiekviena už save, kur jos bando suformuoti savo galias. Apie kibernetinį saugumą kalbant iš tarptautinių santykių studijų perspektyvų, tai, kad viena šalis gali vykdyti kibernetines atakas prieš kitą, nepalikdama jokių konkrečių pėdsakų ir įrodymų, kartu su ribotomis prevencinėmis priemonėmis sąlygos visiško tarptautinio nepasitikėjimo vieni kitais ir tarptautinėmis institucijomis būsenos susiformavimą. Iš esmės realizmas sprendžia skaitmeninio amžiaus problemas kaip ir kitus globalizacijos aspektus – juos ignoruodamas arba kategorizuodamas kibernetinį saugumą kaip politinės ekonomikos arba vidaus politikos reiškinį. Vertinant iš strateginių studijų perspektyvos, egzistuoja klasikinio realizmo mokyklos atstovų idėjos, kurios informacinį karą, kuris, jų nuomone, yra technologinis klasikinio psichologinio karo formų tęsinys, mato kaip vieną esminių konceptų šioje tyrimų srityje. Nepaisant to, kad informacinio karo plėtotės skalėje toliau eina elektroninis karas, bendroji šių priemonių analizė neišeina iš karinės ir valstybinės perspektyvų ribų (Eriksson ir Giocomello, 2006). Pagrindinė realistinio požiūrio problema yra ta, kad šios mokyklos atstovai vertindami nagrinėjamų viena prieš kitą priešpriešą vykdančių sistemų veikėjus, pagrindinį dėmesį skiria valstybėms, tačiau neįvertina nevalstybinių veikėjų vaidmens. Toks požiūris galbūt ir tinkamas nagrinėjant konvencinius konfliktus, kur valstybė turi turėti pakankamų resursų vykdyti priešpriešą prieš kitą valstybę, tačiau kibernetinio saugumo kontekste nėra pakankamai efektyvus, nes bet koks individas, interesų grupė ar organizacija, esanti tinkle, gali vykdyti atakas prieš kitą

individą, organizaciją ar net prieš visą valstybę ir taip sąlygoti sisteminius pažeidimus bei žalą. Kibernetinio konflikto priemonės savo prigimtimi, lyginant jas su konvencinio karo atributais, yra asimetriškos, mažiau apčiuopiamos, o pats kibernetinis karas yra labiau panašus į partizaninį, lyginant jį su klasikiniais, istoriniais mūšiais, arba valstybių apsikeitimu branduoliniais smūgiais hipotetiniame konflikte (Barlow, 2010). Gynybiniai ir puolamieji realistai teigia, kad pirmojo smūgio sudavimas yra pats tinkamiausias būdas išspręsti saugumo dilemą ir užtikrinti, kad priešas neatsakys tuo pačiu. Tačiau kibernetinio konflikto kontekste to padaryti neįmanoma, nes prognozuoti rengiamas atakas nėra galimybių, o vienintelis būdas užkirsti kelia priešiškai valstybei atsakyti į ataką yra jos infrastruktūros atjungimas nuo bendro interneto tinklo, kas yra neįgyvendinamas uždavinys. Tokiu būdu, du konfliktuojantys vienetai gali nuolatos keistis kibernetiniais smūgiais, pridarydami vienas kitam nuostolių, tačiau apie visišką kažkurios pusės sutriuškinimą kalbėti būtų sudėtinga. Be to, diskutuotinas ir atgalinio smūgio (angl. *hack-back*) etiškumo klausimas. Atsakomoji ataka (angl. *hack-back*) – bandymas atsakyti kompiuteriniam įsilaužėliui, atakuojančiam sistemą, tuo pačiu, laikoma nelegalia veikla, net tuomet, kai yra žinomas atakos kaltininkas (Ayala, 2016). Atsakomosios atakos konceptas reiškia įsilaužėlių identifikavimą ir pavogtų duomenų sunaikinimą. Kartais jis yra svarstomas, tačiau kibernetinio saugumo ekspertai dažnai perspėja apie tokių veiksmų pasekmes, pradedant galimybe pažeisti legalumo ribas, baigiant – iššaukti didžiulio masto kibernetinius konfliktus, kurie sąlygotų didžiules kibernetinės priešpriešos apraiškas, atnešančias sunkiai nusakomo masto griaunamus efektus, darančius tiesioginį ar šalutinį poveikį visai kibernetinei erdvei (Holzer ir Lerums, 2016). Atskirai vertėtų pažymėti, kad dėl aiškiai matomų ir jaučiamų pasekmių niekam nekiltų abejonės, ar branduolinis karas yra įvykęs ir, kuri konfliktuojanti pusė jį pradėjo ir todėl yra atsakinga už jį ir visus jo padarinius, tačiau kibernetinės priešpriešos atveju, kai konflikto technologijos nėra fiziniai vienetai, egzistuoja daugybė būdų atakas vykdyti nepastebėtai ar bent jau išvengiant identifikacijos. Dažniausiai dėl šios priežasties šias atakas įvykdžiusios valstybės gali teigti, kad jos su konkrečiomis atakomis yra nesusijusios.

Kritikuojantys realistus pažymi, kad jų taikomos teorijos naudoja pernelyg siaurą nacionalinio saugumo matymą, sukoncentruotą ties fizinių sienų apsauga ir strateginių vertybių apsaugojimu nuo užsienio valstybių karinių atakų. Taikant platesnį požiūrį, numatomas ne tik teroristinių atakų pavojus, galintis kilti valstybės viduje, tačiau ir visos galimos ne vien karinės prigimties grėsmės. Vienas iš požiūrių, metantis iššūkį realistų grėsmės matymui yra Kopenhagos saugumo studijų mokyklos atstovai, siūlantys konceptualių skirtumų tarp kibernetinio ir kompiuterių saugos domenuose vyraujančio saugumo suvokimo. Kopenhagos mokyklos atstovai nesistengia objektyviai charakterizuoti grėsmes, pažeidžiamumus ir gynybos modelius, vietoj to, jie siūlo taikyti sisteminį požiūrį, pagal kurį, esant tam tikroms specifinėms sąlygoms, konkrečiai padėčiai ar įvykiams, kyla grėsmė saugumui ir šis pats grėsmės faktas yra plačiai pripažįstamas reikšmingų socialinių veikėjų. Tokį grėsmės vertinimą Kopenhagos mokyklos atstovai siūlo spręsti saugumizacijos priemonių pagalba (Nissenbaum 2005).

Liberalizmas. Moravcsik (2001) išskyrė idėjinį (angl. *ideational*), komercinį ir respublikoniškąjį liberalizmą, Doyle (1998) suformavo teorinius tarptautinio, komercinio ir ideologinio liberalizmo aspektus, Zache ir Matthews (1995) pateikė savas liberaliosios

saugumo minties idėjas (Navari, 2008). Pasak Eriksson ir Giocomello (2006), pats ryškiausias liberaliosios teorijos indėlis į tarptautinių santykių discipliną gali būti įvardijamas keturiais pagrindiniais elementais: tarptautinių veikėjų pliuralizmo pabrėžimas; vidinės politikos svarba nulemiant tarptautinę valstybių elgseną; tarptautinių institucijų vaidmuo nustatant valstybės veikėjų elgseną; tarptautinių studijų darbotvarkės praplėtimas, koncentruojantis į platesnius klausimus nei tiesiog klasikinio hobizmo apimamą anarchistinę tarptautinę aplinką. Liberalioji kryptis, priešingai nei realistai, pripažįsta, kad valstybės nėra centriniai pasaulinės politikos veikėjai, o tai labiau atitinka pastarųjų laikų tarptautinės politikos realijas, kai tarptautinių santykių srityje daugėja nevyriausybinių tarptautinių veikėjų: tarptautinių korporacijų, socialinių judėjimų, lobistinių grupių, politinių partijų tinklų, emigrantų ir teroristų. Neretai visos šios grupės savo komunikacijai bei veiklai vykdyti pasirenka elektroninių medijų pagrindu veikiančias technologijas, tad iš esmės liberalizmas pripažįsta bet kokių įtinklintų grupių atsiradimą.

Konstruktyvizmas. Vėlyvaisiais 1980-aisiais konstruktyvizmas buvo integruotas į tarptautinių santykių studijas. Nuo to laiko konstruktyvizmo svarba ženkliai išaugo tarptautinių santykių studijų lauke, jis įnešė ryškų indėlį šios srities teorijos formavimo ir empirinių tyrimų srityje (McDonald, 2008). Pagrindinė konstruktyvizmo mokyklos atstovų idėja yra požiūris teigiantis, kad saugumas yra socialinis konstruktas. Tokiu būdu, saugumas gali būti suvokiamas kaip tam tikros grupės pamatinių vertybių išsaugojimas, nors toks apibrėžimas nedetalizuoja, kas yra toji grupė bei kokios yra jos pamatinės vertybės ir, kaip gali būti pasiektas jų išsaugojimas (McDonald 2002). Konstruktyvistams atsakymai į šiuos klausimus skirtinguose kontekstuose yra skirtingi ir susiformuoja per socialinę interakciją tarp veikėjų. Konstruktyvistai vieningai sutaria, kad nėra vieningo, universalaus, abstraktaus saugumo apibūdinimo (Williams, 2008). Konstruktyvistinės saugumo studijos įnešė pakankamai didelį indėlį į saugumo koncepto detalizavimą ir nubrėžė sąsajas tarp saugumo politikos ir nacionalino identiteto (Buzan ir kt., 1998). Vienas ryškesnių konstruktyvistų indėlių į saugumo studijas yra jau minėtos Kopenhagos saugumo mokyklos saugumizacijos teorijos suformavimas. Kelios kitos konstruktyvistų idėjos, susijusios su skaitmenine erdve, nagrinėja kaip informacinė priešprieša kelia grėsmę identiteto suvokimui. Everard (2000) teigia, kad informacinis karas yra iš esmės identitetų karas, kuriame metamas iššūkis visoms nustatytoms riboms, taip pat ir egzistuojančioms klasikinėms vidinio tarptautinio pasidalijimo riboms. Patirdama informacinio karo iššūkius valstybė yra nuolatiniame nacionalinio identiteto nuginčijimo pavojuje, tačiau ji gali gerai adaptuotis ir nepasiduoti nuolatinėms jos formalioms suverenioms sienų ir vertybių riboms kylančioms grėsmėms kibernetinėje erdvėje (Saco, 1999). Konstruktyvistai, nagrinėdami galios ir saugumo konceptus virtualioje erdvėje, pažymi būtinybę pabrėžti ne tik materialios realybės atributų kompiuterių ir tinklų, bet ir simbolių bei vaizdinių svarbą. Kaip pažymi Der Derian (2000), dėl savo panašumo į simuliaciją ir kompiuterinius žaidimus viena iš priešpriešos skaitmeninėje erdvėje ypatybių yra ta, kad joje dalyvaujantys veikėjai yra savo suvokimu, mentališkai atitolę nuo kruvinųjų tikrojo karo realijų. Tokį atitolimą dar pagilina ir tai, kad visi priešpriešos veiksmai yra vykdomi kompiuterių pagalba, t.y. už tam tikras veikas atsakingam asmeniui ar asmenų grupei neturint jokių sąsajų su savo veiklos objektu. Tai sąlygoja tokią būseną, kai ištrinamos ribos tarp realaus ir įsivaizduojamojo, virtualaus

pasaulio. Kalbant apie virtualias erdves, pažymėtina, kad jos yra puiki terpė per simbolius manipuliuoti viešąja nuomone bei politiniu diskursu, todėl ši sritis yra ypač aktuali nagrinėti ją iš skaitmeninio saugumo perspektyvų, taikant Edelman (Edelman, 1977, 1985) ir kitų konstuktyvistų suformuotus simbolių politikos požiūrius. Iš simbolių politikos studijų perspektyvos, taikant ją kibernetinėje erdvėje, atakos prieš konkrečių šalių valstybinius tinklalapius ar korporacijas, nors dažnai ir neatneša didelių nuostolių ir niekam nekelia realios politinės grėsmės, tai yra simbolių politikos tąsa virtualioje erdvėje ir matomos kaip nacionalinių vertybių įžeidimas. Pagal Eriksson ir Giocomello (2006), simbolizmas ir abstrakcija yra perkeliami į informacinio saugumo terminiją, sugalvojant analogus realaus pasaulio objektams. Tokio reiškinio pavyzdžiai yra: virusai, kirminai, ugniasienės, informaciniai karai, „elektroninis Perl Harboras". Būtent toks abstrahavimas, paremtas realaus pasaulio terminais padeda geriau suvokti virtualiame pasaulyje vykstančių įvykių pasekmes.

Kaip pažymi Eriksson, Giocomello (2006), liberalizmo ir konstruktyvizmo mokyklos matomos kaip galinčios duoti teigiamą impulsą kibernetinio saugumo teorijos formavimui, ypač tai tampa akivaizdu pašalinus iš liberalizmo idealistines ir antirealistines potekstes. Liberalizmas palaiko tokias idėjas, kaip nevyriausybines organizacijas atstovaujančius, gebėjimus veikti tarptautinėse sistemose turinčius veikėjus, tinklo ekonomiką. Konstruktyvizmo mokykla, savo ruožtu, yra linkusi analizuoti simbolinius, retorinius ir identitetu pagrįstus kibernetinio saugumo aspektus. Eriksson ir Giocomello (2006), nagrinėdami kibernetinio saugumo teorijas, siūlo jas visas integruoti ir suformuoti tarpinę, liberalizmą, konstruktyvizmą ir realizmą integruojančią teoriją, kuri padėtų suvokti informacinės revoliucijos metu kylančius iššūkius saugumui. Jie pažymi, kad specializuota literatūra saugumo srityje yra ganėtinai stipriai orientuota į politikos formavimo procesus ir su ypač retomis išimtimis bando nagrinėti saugumo problemas iš skaitmeninio amžiaus perspektyvų.

Kopenhagos mokyklos atstovai suformavo pakankamai tvarų teorinį pagrindą nagrinėti grėsmes saugumui, tačiau ilgainiui atsirado poreikis šį kontekstą papildyti ir naujai konceptualizuotomis idėjomis, padėsiančiomis iš grėsmės perspektyvų įvertinti ir kibernetinius pavojus. Tradicinėje saugumo studijų literatūroje skiriama aibė nacionalinio saugumo elementų, formuojančių bendrąją valstybės nacionalinio saugumo sistemą: karinis, politinis, ekonominis, socialinis, aplinkos (Buzan, Wæver, Wilde, 1998). Vėliau prie šių elementų buvo siūloma pridėti ir komunikacijų saugumo elementą (Hansen ir Nissenbaum 2009; Lobato ir Kenkel 2015) – tai atspindi konkrečiu momentu susiformavusią būtinybę praplėsti saugumo studijų disciplinoje nagrinėjamų saugumo elementų sistemas. Akademinėje saugumo studijų bendruomenėje vieni ankstyvesnių bandymų atsakyti į kibernetinėje erdvėje kylančių grėsmių sukeliamus iššūkius nacionaliniam saugumui buvo Yold (2003) iškelta idėja, kad IRT gali būti bendrinis, visų saugos sektorių konvergencijai pagrindą formuojantis elementas. Toks praplėstas saugumo sektorių požiūris leistų kibernetinės saugos kontekstui taikyti Kopenhagos saugumizacijos modelį bei, kas labai svarbu kibernetinio saugumo atveju, atskirti saugumizaciją nuo militarizacijos, praplėsti šio domeno diskursą ir vertinti patį saugumą ir visus jo sektorius per nacionalinio saugumo prizmę (Wæver, 2011) visiškai nauju aspektu. Nemažai prie požiūrių į kibernetinį saugumą plėtros prisidėjo ir Nissenbaum (2005), kuris saugumą analizavo iš dviejų skirtingų konceptų pjūvių. Visų

pirma, tai techninis – kompiuterijos ir tinklų saugumas, susijęs su įvairiais inžinerijos ir kompiuterijos aspektais, antra, tai saugumas iš už saugą atsakingų nacionalinių valdžios institutų perspektyvos. Būtent antrasis matymas pakylėja kibernetinio saugumo svarbos lygmenį, suteikdamas valstybinės svarbos reiškinio statusą. Taigi kibernetinio saugumo koncepto susiformavimas bei vykstanti jo artikuliacija valdžios institucijose, korporacijose ir nevyriausybinėse organizacijose sąlygojo kompiuterijos saugumo bei tradicinio nacionalinio saugumo sąsajų atsiradimą. Įvykusi šių dviejų konceptų sanglauda, sąlygojo būseną, kai jie egzistuoja vienas šalia kito, apjungdami esminių socialinės srities veikėjų, tokių kaip valdžios institucijos, techniniai ekspertai, korporacijos, politikos ekspertai, akademinė bendruomenė, visuomenė bei visų formų žiniasklaida (Nissenbaum, 2005).

Apibendrinant pažymėtina, kad kibernetinės saugos konceptualizavimo dėka iš nacionalinio saugumo perspektyvos tradicinės informacinių sistemų saugos konceptas išplėtojamas į bendravalstybinį saugumo reiškinį, į kurio veiklos sritis patenka visas valstybės kompiuterinis tinklas, kuriame veikia kritinė valstybės informacinių sistemų infrastruktūra, į kurį yra prisijungusios valstybinės ir privačios organizacijos, eiliniai vartotojai. Tokiu būdu, kibernetinės erdvės apsauga tampa nacionalinio saugumo ir teisėsaugos sistemų dalimi, ypač atsižvelgiant į tai, kad nepaisant, jog nusikalstamos ar prieš valstybę nukreiptos veiklos yra vykdomos elektroninių priemonių pagalba, jų pasekmės peržengia kibernetinio pasaulio ribas.

Kibernetinės erdvės saugumizacija. Kibernetinio saugumo transformacija nacionalinio saugumo kontekste būtų nepilna neišnagrinėjus jos saugumizacijos modelio perspektyvoje, kuri padeda praplėsti kibernetinės grėsmės suvoktį. Nagrinėjant grėsmės sąvokas, be galo svarbu atsakyti ir į klausimą, kas yra saugumas iš nacionalinio saugumo perspektyvos. Ko gero, politiniame diskurse vieni dažniausiai visuomenės ir politikų užduodamų klausimų: „Ar mūsų visuomenė, aplinka, valstybė yra saugios?“. Be to, diskutuojant iš Shamir pasiūlytos trijų saugumo dėsnių prizmės, kurių vienas teigia, kad jokia sistema nėra absoliučiai saugi (Shamir, 2002), kyla papildomi klausimai: koks maksimalus saugumo lygis yra pasiekiamas ir koks yra toleruotinas. Nagrinėjant Kopenhagos mokyklos idėjas, pažymėtina, kad jos apskritai nėra koncentruojamos ties aktualiomis grėsmėmis, su tuo susijusiais objektais, gynybiniais manevrais ar panašiomis tradicinio konflikto priemonėmis, o veikiau yra sutelktos ties grėsmių atvaizdavimu saugos kontekste bei jų įprasminimu. Taip, iš tradicinio saugos koncepto nacionalinio saugumo domene vyksta vertinimo poslinkis nuo paradigminio karinio grėsmių suvokimo link labiau bendrinės sampratos. Bandydami teorizuoti šias grėsmes Kopenhagos mokyklos atstovai pasiūlė saugumizacijos (angl. *securitization*) sąvoką, kuri suprantama kaip „procesas, kurio metu valstybinio mąsto veikėjai transformuoja tam tikrą subjektą į saugumo klausimą: tai ekstremali politizavimo forma, įgalinanti ypatingų priemonių taikymą saugumo vardan“ (Buzan, Wæver, Wilde, 1998). Pagal saugumizacijos teoriją grėsmės atvaizduotinos ne vien tik paprasčiausiai kenksmingomis, bet žūtbūtinėmis, neišvengiamomis ir egzistencinėmis. Grėsmė turi būti pateikiama visuomenei ir tos visuomenės pripažįstama fatalia jos vertybinės visumos objekto visuotinei egzistencijai. Tai yra gyvenimo ir mirties klausimai egzistencinės grėsmės grupei, subjekto vertei, jo pasirinktos gyvensenos būdui ar ideologijai (Buzan, Wæver, Wilde,

1998). Kai kurių autorių nuomone, kibernetinis saugumas apibendrintai gali būti matomas kaip kompiuterinė sauga, praplečiama saugumizacijos konceptu (Hansen, Nissenbaum 2009). Saugumizacijos procesas apima keturis pagrindinius aspektus:

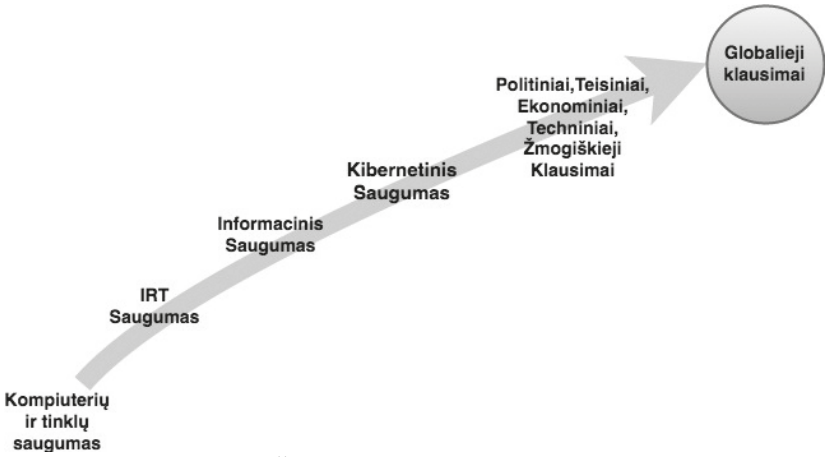
- saugumizuojantis veikėjas (agentas) – subjektas, inicijuojantis saugumizacijos procesą;
- egzistencinė grėsmė – potencialiai keliančiu grėsmę identifikuojamas objektas;
- referentinis objektas – objektas, kuriam kyla grėsmė, kuris turi būti apsaugotas;
- visuomenė (angl. *audience*) – grėsmę saugai paskelbiantis ir saugumizaciją vykdyti įtikinantis subjektas (Buzan, Wæver, Wilde, 1998).

Saugumizacijos konceptas generalizuoja tam tikrus tradicinio požiūrio į nacionalinį saugumą aspektus, kuriame tipinis kontekstas apima karinės atakos grėsmės pavojų, valstybę, susiduriančia su grėsme, bei specifinius žingsnius, kurių imasi lyderiai, siekiantys užtikrinti tęstinę saugos būseną, taikant tokias priemones kaip gynybiniai veiksmai, pažeidžiamų vietų stiprinimas ir kitus panašaus pobūdžio veiksmus. Valstybės atveju saugumizuojama grėsmė yra ta, kuri primetant svetimą valią kelia pavojų nacionaliniam suverenitetui, politinei autonomijai, kultūriniam identitetui, socialinei santvarkai, istoriškai susiformavusiam gyvenimo būdui, tradicijoms. Labai svarbus Kopenhagos modelio aspektas – agentas. Tai yra subjektas, kuris turi teisę ir galimybes saugumizuoti ir būti saugumizuojančiu veikėju. Tai dažniausiai apima aukšto rango išrinktus arba paskirtus valdžios atstovus, vyriausybę, aukšto rango karinių struktūrų atstovus, prezidento instituciją. Tap pat įmanoma, kad ir kitos visuomenės ar valstybinės grupės, tokios kaip patikimi medijos resursai, teisininkai ar iškilūs korporacijų atstovai, gali pasiekti pakankamą įtikinimo potencialą grėsmės konceptualizavimui, kuris būtinas saugumizacijai. Pagal Deibert (2002 iš Hansen, Nissenbaum, 2009), kibernetinės saugos kontekste saugumizavimas taikytinas kelioms kategorijoms. Visų pirma, tai – internetas, kaip komunikacijos kanalas, ir jo pagrindu veikiančios naujosios medijos, suteikiančios galimybę jų naudotojams vykdyti komunikaciją vienas su vienu, vienas su daugeliu, daugelis su daugeliu. Kita kategorija yra tiesiogines, katastrofiškas, dramatiškas pasekmes turinčios kibernetinės atakos ir išpuoliai prieš kritinę infrastruktūrą. Deibert (2002 iš Hansen, Nissenbaum, 2009) pažymi, kad skaitmeniniai tinklai yra referentiniais objektais, kuriems kyla saugumo grėsmės, sisteminės saugos spragos, jais perduodamų duomenų sugadinimas bei informacinių srautų pertraukimas. Visi šie aspektai gali būti patys suvokiami kaip atskiri referentiniai objektai. Toks suvokimas sąlygoja socioekonominį ir politinį struktūrinių pažeidimų matymą, o vieši ir privatūs subjektai vienodai gali būti pažeidžiami kibernetinių atakų ir patys gali būti jų kaltininkais. Deibert (2002 iš Hansen, Nissenbaum, 2009) manymu, tinklų sauga yra ne tik referentinis objektas kibernetiniame sektoriuje, bet ir kitų referentinių objektų formavimo pagrindas. Šiuolaikiniame kibernetinių pavojų kontekste tinklas tapo potencialiu karo lauku ir terpe vykdyti išpuoliams, neretai nukreiptiems prieš ištisas valstybes. Priešiški veiksmai vykdomi elektroninėje erdvėje naudojant kompiuterinius virusus, kirminus bei kitą kenkėjišką programinę įrangą, galinčią pasitarnauti priešiškos valstybės strateginių tikslų pasiekimo procese, sutrikdant prieigą arba galios koncentraciją ir tėkmę tam tikrose jautriose srityse. Kibernetinės atakos gali būti nukreipiamos prieš nacijas, kolektyvinį identitetą turinčius subjektus, suvokiant juos kaip pirminius referentinius objektus. Kai

kurios šalys, pavyzdžiui, Kinija ir Iranas, mano, kad jų kolektyviniam identitetui kyla grėsmė dėl besiplėtojančios prieigos prie interneto (Nissenbaum, 2005). Pagal Nissenbaum (2005), bandant apibrėžti kontrastus ir suvokti kaip saugumas tarnauja konceptualiu pagrindu informacinių sistemų saugai ir kibernetiniam saugumui, būtina suvokti, radikaliai skirtingus kibernetinio saugumo sudėtingumo laipsnius ir grėsmių prigimtį. Kontrastuoja ir grėsmių bei grėsmių tipų suvokimas, apimantis pavojus kylančius nuosavybei, išpuolius prieš autonomiją, privatumą ir produktyvumą. Saugumizuojant grėsmes, skirtingai nustatomas jų pavojingumas ir egzistencijos laipsnis. Kitas labai svarbus kontrastas yra prototipinio referentinio objekto nustatymas. Ilgą laiką egzistavęs technokratinis požiūris saugumo grėsmę mato visų pirma individams, agentams ar institucijoms, vėlesnis požiūris koncentruojasi į kolektyvinę saugą, apimančią valstybės ar nacijos ribas (Nissenbaum, 2005). Trečiasis kontrastas, išreiškiamas per moralinių galių kaupimo šaltinį, t.y. per tai, koks pagrindimas naudojamas imantis vienų ar kitų veiksmų saugumui užtikrinti, t.y. šių veiksmų moralinio pagrindo formavimas. Tradicinis techninis informacinių sistemų saugumas apima saugos priemonių diegimą, kuriuo siekiama apsaugoti tinkle esančius individus ar institucines sistemas, taikant technines apsaugos nuo grėsmių priemones. Šio pobūdžio saugumas nėra nukreiptas identifikuoti ir sustabdyti potencialius užpuolikus iki jie imsis konkrečių neteisėtų veiksmų – tai labiau į potencialių taikinių apsaugos stiprinimą orientuotas būdas (Nissenbaum, 2005). Kalbant apie techninio kibernetinio saugumo suvokimo ribotumą, pažymėtina, kad kompiuterių ir įtinklintos saugos kontekste grėsmių analizei reikalingi duomenys ne visuomet yra prienami visuomenei. Tai yra viena iš pagrindinių priežasčių, dėl kurios dauguma aukščiausio rango technologijų saugos ekspertų vykdo tyrimus technologinių pažeidžiamumų srityje, nagrinėdami galimų atakų galimybes ir jų sukeliamą žalą, taip nematydami holistinės jų tikimybės bei jų veikimo masto perspektyvos. Kaip pažymi Nissenbaum (2005), būtent tokios perspektyvos ugdymas reikalauja daugiau nei elementaraus techninio, analitinio suvokimo. Fragmentuota informacija apie atsitiktines atakas negali būti pagrindu formuojant išsamias išvadas, galinčias tapti indėliu darant pasirinkimą iš techninės ar kibernetinės saugos sprendimų. Tik iš vienpusės, siauros, techninės perspektyvos įvertinta informacija nesudaro galimybės strategiškai įvertinti ir suprasti problemos bei pažeidimų masto. Virusinė ataka internete, dėl kurios pažeidžiama aibė kompiuterinių sistemų, interpretuojant ją iš techninės perspektyvos, gali būti suprantama kaip kriminalinė veikla prieš didelį skaičių asmenų – ir tai yra vidaus reikalų srityje teisėsaugą įgyvendinančių institucijų kompetencija, įgyvendinama vykdant tyrimus ir kitus teisinius veiksmus. Tokia pati ataka, vertinant ją iš kibernetinės saugos modelio perspektyvų, gali būti atitinkamai laikoma ataka prieš naciją ir suvokiama kaip saugumizacijos pavyzdys (Nissenbaum, 2005). Eriksson (2001) atliko Švedijos informacinių technologijų saugumizacijos analizę, kurios metu, nustatė skirtingų su IRT susijusių grėsmių konceptualizavimo poveikį jų suvokimui. Taip, konceptualizuojant incidentą kaip kibernetinį nusikaltimą, atsiranda suvokimas, kad jis yra atliktas nusikaltėlių, todėl šio nusikaltimo išaiškinimas turėtų būti policijos atsakomybė. Nors lygiai tas pats incidentas gali būti konceptualizuojamas kaip informacinis karas, kas sąlygoja suvokimą, kad už šio nusikaltimo įvykdymą atsakinga priešiška valstybė, valstybinės ar nevalstybinės grupės, o taip konceptualizuoto nusikaltimo atveju, į jį atsakyti turėtų karinės pajėgos (Bendrath,

2001; Eriksson, 2001). Konkretaus suvokimo svarba pasireiškia tuomet, kai, pavyzdžiui, reikia įvertinti vykdomus kibernetinius išpuolius prieš nacionalinės svarbos tinklalapius ar strateginės infrastruktūros sistemos dalis. Suvokiant šį reiškinį iš technologinės perspektyvos, tai tėra kriminalinė programišių veikla, tačiau iš kibernetinės saugos perspektyvos – tai gali būti išpuolis prieš valstybę, kuris turi būti vertinamas saugumizacijos požiūriu (Nissenbaum, 2005).

Apibendrinant skyrių galima Ghernaouti (2013) idėjomis, kad šiuolaikiniai elektroninėje erdvėje esantys iššūkiai yra apimantys technologines, žmogiškąsias ir ekonomines skaitmeninės infrastruktūros dimensijas, todėl jų sprendimas reikalauja tarpdisciplininio požiūrio taikymo ir tai nėra vien tik informacinių technologijų srities problema.



Šaltinis: *Ghernaouti (2013)*

6 pav. *Saugumo diskurso klausimų dinamika*

Dėl savo kompleksiškumo ir poreikio taikyti visa apimančius strateginius požiūrius ši sritis turi būti integruojama į socialinių, ekonominių ir viešosios politikos klausimų dienotvarkę. Be to, pats kibernetinio saugumo procesas įtakoja visą visuomenę. Konceptualizuojant šias idėjas ir atvaizduojant jas grafiškai, galima būtų visus su technologiniais klausimais susijusias saugumo veiklas atvaizduoti saugumo konceptualios plėtotės vektoriaus pradžioje – vektoriaus kryptis yra politiniai, ekonominiai, techniniai, žmogiškieji klausimai, kurie galiausiai įsilieja į globaliuosius visos žmonijos klausimus, tokius kaip globalizacija, ekologija ir kt.

1.5. Atsparumo diskurso aktualizavimas

Kaip pastebi Flynn (2011), XI a. klestės tik atsparios bendruomenės, organizacijos ir šalys. Terorizmas, epidemijos, klimato kaitos sukeltos katastrofos bei nuolatiniai sudėtingų ir tarpusavyje priklausomų tinklų veiklos sutrikdymai taps įprastais reiškiniais. Tad sociotechniniai junginiai kurie gali atlaikyti, duoti atsaką ir atsistatyti bei adaptuotis

prie rizikų turės ryškų pranašumą prieš tuos, kurie to padaryti negali. Gibson ir Tarrant (2010) pažymi, kad pastaraisiais dešimtmečiais nepastovumas natūraliose, ekonominėse ir socialinėse sistemose didėja tokiu greičiu, kad dauguma organizacijų, kurios yra įpratusios veikti rutininėse, stabiliose bei lengvai prognozuojamose aplinkose, tokių pokyčių tiesiog nepajėgia tinkamai valdyti, taip įgaudamos didelio masto pažeidžiamumą. Pastaruoju metu, nepastovumas ir neužtikrintumas tampa organizacijų išorinių ir vidinių operacinių aplinkų norma. Vis labiau tampa aktualiu poreikis ieškoti būdų, kaip galima būtų atsakyti į tokio nepastovumo keliamus iššūkius, padėsiančius organizacijoms ne tik efektyviai vykdyti operacijas, bet apskritai išgyventi. Identifikuoti, ką reiškia būti atspariu bei organizuoti veiklas remiantis šiomis žiniomis, taps būtina sąlyga siekiant augimo ir saugumo globalioje aukštą įtinklinimo lygį turinčioje bendruomenėje (Flynn, 2011). Kaip pažymi Welsh (2014), kompleksiškame nenumatytų atvejų, rizikų, reliacijų, įvairiakrypčių srautų ir kintamumų pasaulyje ypač patraukliai atrodo metodikos, kurios pateiktų priemonių rinkinį, galinčių suteikti teorinių instrumentų rinkinį kompleksiškumui suvaldyti. Atsparumas yra viena tokių teorijų, kuri pastaruoju metu taikytina šiems iššūkiams spręsti, visur esantis (angl. *ubiquitous*) reiškinys, skirtas sudėtingoms (angl. *complex*) sistemoms bei juose vykstantiems procesams bei jų kaitos efektams suvokti. Atsparumo pagrindą sudaro fundamentinis rizikų suvokimas ir jų valdymas, ypač tai taikytina nerutininių rizikų ar sisteminių žlugimų atveju (Gibson ir Tarrant, 2010). Reikia pastebėti, kad plačiai vartojamas ir vertinamas kai kuriose šalyse, pavyzdžiui, JAV, atsparumo konceptas tik pakankamai nesenai yra pradėtas taikyti žemyninėje Europos dalyje. Todėl dėl šio reiškinio nepakankamo apibrėžtumo vis dar pakankamai sudėtinga jį įgyvendinti, šiuo metu jis vis dar išlieka labiau pradinis idėjinis lygmuo, nei teorinį pagrindą turintis konceptas (Joseph, 2013). JAV atsparumo sąvokos formavimasis, prasidėjęs didelio patikimumo organizacijų teoriniame domene su Sutcliffe ir Vogus (2003) organizacinio atsparumo idėjomis. Vykęs palaipsniui, organizacinio atsparumo plėtojimasis tapo logišku egzistuojančių rizikų ir sistemos saugumo vertinimo trūkumų sukeliamų iššūkių sprendimu. Sutcliffe ir Vogus (2003) bendrine prasme apibrėžia atsparumą kaip pozityvų organizacijos prisitaikymą (angl. *adjustment*) iššūkius keliančiomis sąlygomis. Nagrinėdami konkrečiai organizacinį atsparumą kaip reiškinį, tyrėjai skiria dvejopas atsparumo suvokimo kryptis. Visų pirma, tai gebėjimas absorbuoti įtampą (angl. *strain*) ir išsaugoti arba net pagerinti organizacijos funkcionavimą nepaisant nepalankių sąlygų (angl. *adversity*). Kalbėdami apie nepalankias sąlygas, Sutcliffe ir Vogus (2003) skiria vidines, tokias kaip greiti pokyčiai, netinkama lyderystė ir kt., bei išorines, tokia kaip kylantis konkurencijos lygis ir suinteresuotų pusių (angl. *stakeholders*) reikalavimai, sąlygas. Antroji tyrėjų skiriama atsparumo suvokimo kryptis yra gebėjimas „atšokti“ (angl. *bounce-back*) nuo nepageidaujamų įvykių. Besivystant atsparumo teoriniam laukui tam tikru metu egzistavo ir gimininigi jam teoriniai konceptualūs modeliai, vienas tokių – Carlson ir Doyle (1999) suformuotas didelės tolerancijos optimizavimo (angl. *Highly Optimised Tolerance*) modelis, atsiradęs pradėjus nagrinėti fundamentinius sistemų sudėtingumo aspektus. Europoje tyrėjai ir praktikai, atstovaujantys skirtingas disciplinas suvienijo savo jėgas ekspertų grupių formatu – taip atsirado Atsparumo aljansas (angl. *Resilience Alliance*), Atsakymo į krizes ir valdymo informacinių sistemų bendruomenė (angl. *Information Systems for Crisis Response and Management*).

Kalbant apie atsparumo apibrėžimus, pažymėtina, kad jie varijuoja nuo vieno tyrimų lauko iki kito, tačiau vienas dažniausių atsparumo naudojimo pavyzdžių sutinkamas medžiagų ir inžinerijos moksluose medžiagų atsparumo kontekste, kuriame atsparumas matuojamas pagal tai, kokį stresinį poveikį gali atlaikyti medžiaga nesulūžusi arba nepakeitusi savo originalios formos, taip pat, kiek ji veikiama šio streso išlinksta ir, kaip greitai grįžta į savo originalią forma stresui nustojus šią medžiagą veikti. Taigi, atsižvelgiant į tai, atsparumas yra objekto gebėjimas atsilaikyti prieš išorines jėgas, šokus ir sutrikdymus bei gebėjimą greitai sugrįžti į savo pradinę, t.y. įprastinę būseną. Holling (1973), kuris laikomas atsparumo idėjų pradininku, nagrinėdamas ekologinį atsparumą, suformavo vieną pirmųjų šio reiškinio apibrėžimų, apibūdindamas atsparumą kaip „sistemos išsilaikymo (angl. *persistence*) matą ir jos gebėjimą absorbuoti pokyčius bei sutrikdymus ir nepaisant jų išlaikyti vienodą santykį tarp populiacijos arba valstybės kintamųjų". Pagal Fjader (2014), socialiniame, individų ir sistemų kontekste atsparumas apibūdinamas kaip gebėjimas atsilaikyti ir atsistatyti arba „atšokti" (angl. *bounce back*) nuo šokų, sukeltų išorinių padarinių, tokių kaip artimųjų mirtys, darbo praradimas, sunkios ligos – individualiame, ir stichinės nelaimės, teroristiniai išpuoliai, kariniai konfliktai – bendruomeniniame ir visuomeniniame lygmenyse. Fjader (2014) pažymi, kad kalbant apskritai apie socialinių sistemų atsparumą, tikslaus apibrėžimo nustatymas tampa daug sudėtingesnis, nes tokiose sistemose yra gan neaiškios atsparumo įgyvendinimo kryptys. Apskritai socialiniame domene atsparumo taikymas kelia nemažai iššūkių, kadangi nėra bendro sutarimo, kas galėtų būti laikytina normalia būsena, sistemos ar verslo pusiausvyra (angl. *equilibrium*), kuri yra siekiamybė, t.y. kurią reikia išlaikyti arba į kurią reikėtų sugrįžti po sutrikdymo. Dažnai tai yra akivaizdu, kai nagrinėjamas individo, vienos sistemos lygmuo, tačiau tampa daug sudėtingiau suvokiama, kai kalbama apie tokius sudėtingus reiškinius kaip nacija (Fjader, 2014).

Atsparumo apibrėžimas kritinės infrastruktūros kontekste yra gana įvairialypis. Pagal JAV Nacionalinės Infrastuktūros patariamosios tarybos siūlymą, kritinės infrastruktūros atsparumas yra gebėjimas sumažinti sutrikdymo mastą, poveikį ir trukmę. Taip pat, tai yra gebėjimas absorbuoti potencialų trikdomąjį įvykį, prie jo adaptuotis ir (arba) greitai po jo atsistatyti. Pagal tarybą, atspari kritinė infrastruktūra turi tris pagrindines savybes:

- tvirtumą (angl. *robustness*) – gebėjimas išlaikyti kritines funkcijas ir absorbuoti poveikį krizinių įvykių ar sutrikdymų metu;
- resursų valdymo efektyvumą (angl. *resourcefulness*) – gebėjimas pasirengti, atsakyti į krizę ar sutrikdymą, nustatant ir išlaikant adaptyvius gebėjimus ir lankstumą reorganizuoti resursus ir vertybes (angl. *assets*);
- greitas atsistatymas (angl. *rapid recovery*) – gebėjimas grįžti į normalų (įprastinį) operavimo režimą kiek įmanoma greičiau.

Kalbant apie atsparumo apibrėžimą nacionalinio saugumo perspektyvoje, vertėtų išskirti britų ekspertų grupės *Demos* (2010) išleistoje ataskaitoje „Atspari nacija", kurioje teigiama, kad atsparumas nacionaliniame kontekste turėtų būti suprantamas kaip „asmens, bendruomenės ar sistemos gebėjimas adaptuotis, norint išlaikyti patenkinamą funkcionavimo, struktūros ir identiteto lygmenį". Nacionalinio saugumo kontekste atsparumo formavimas reikalauja visapusiškų pastangų, besidriekiančių už nacionalinės jurisdikcijos ir konvencinės saugos ribų. Nepriklausomai nuo to, ar valstybė turi adaptuotis pagal klimato kaitą,

kitus gamtinius kataklizmus ar tiesiog plėtrai (Flynn, 2011). Taip pat kai kurie autoriai skiria paslaugų ir vertybių atsparumą, kuris pasiekiamas formuojant bendrą atsparumo valdymo sistemą (Allen ir kt., 2011). Pakankamai didelė dalis atsparumo konceptų nagrinėjami literatūroje, susijusiose su katastrofomis ir nepaprastų situacijų valdymu. Atsparumą katastrofoms Tierney ir Bruneau (2007) įvardino kaip „socialinių vienetų gebėjimą sušvelninti pavojus, turinčius katastrofų požymius bei atlikti atsistatymo veiklas tokiais būdais, kad būtų sumažinami ardomieji padariniai sociumui bei sušvelninami ateities katastrofų galimi padariniai". Ekologinių sistemų kontekste atsparumas paprastai reiškia sistemos gebėjimą atlaikyti griaunančias rizikas nenustojant funkcionuoti. Organizacijų ir veiklos tęstinumo perspektyvoje atsparumas reiškia gebėjimą grįžti į pradinę veiklą po išorinio šoko. Dar kitame kontekste atsparumas gali reikšti perėjimą iš vienos būsenos į kitą, pavyzdžiui, iš karo į taikos ir atgal, išlaikant kertines vertybes ir socialinę sanglaudą (Flynn, 2011). Bishop ir kt. (2011) koncentravosi į atsparumo apibrėžimo suformavimą ir jo sąsajų su stiprumo (angl. *robustnes*) bei išlikimo (angl. *survivability*) konceptais paieška, taip pat pažymėjo atsparumo ryšius su kitais saugumo sistemos komponentais – konfidencialumu ir integralumu.

Bendras faktorius visiems koncepto pritaikymams yra psichologinės ar fizinės traumos, pažeidimo arba krizės atsiradimas, paveikiantis centrinį subjektą ir neigiamai įtakojantis jo veiklą. Tai gali būti ekosistema, asmuo, ekonominis regionas, sistema, organizacija. Atsparumas, visų pirma, suvokiamas kaip savybė, kuri apima subjekto gebėjimą numatyti, adaptuotis ir atsistatyti po tam tikro įvykio, taip, kad būtų atstatoma originali subjekto konfigūracija, forma, funkciniai ryšiai ir kitos savybės (Welsh, 2014). Savo fundamentine prasme atsparumas yra diskursas apie žmogaus saugumą sudėtingame įtinklintame pasaulyje (Welsh, 2014). Gibson ir Tarrant (2010), suformavę principinį atsparumo modelį, siūlo atsparumo tyrimams pagrindą sudarančių šešerių principų rinkinį, sugeneruotą iš skirtingose atsparumo pakraipose taikytinų įvairiose tyrimų disciplinose:

- Atsparumas yra rezultatas (angl. *outcome*) – atsparumas pagal autorius nėra procesas, valdymo sistema, prognozavimo instrumentas. Jo negalima lyginti su veiklos tęstinumu ar nepaprastų situacijų valdymu, nors abu šie reiškiniai gali būti svarbūs faktoriai, darantys atsparumo reiškiniui reikšmingą įtaką. Atsparumas laikytinas bruožu, kuris gali būti stebimas atsako į esminę aplinkybių kaitą metu.
- Atsparumas nėra statinis bruožas – nėra metrikos ar mato, kuris paaiškintų atsparumą kaip fiksuotą bruožą. Organizacijos atsparumas jokiais būdais negali būti nuolatinis – tai dinaminis elementas, kuris kis priklausomai nuo neapibrėžtumo laipsnio išorinėje aplinkoje bei pokyčio konteksto ir kaip bendrieji organizacijos gebėjimai pasikeis laikui bėgant.
- Atsparumas nėra vienintelis (angl. *single*) bruožas – jis susiformuoja iš kompleksiškos įvairių faktorių sąveikos. Keičiantis aplinkybėms, visų šių faktorių buvimas, svarba ir indėlis atsparumui taip pat keisis.
- Atsparumas yra multidimensinis – tyrėjų manymu, nėra nei vieno modelio, kuris visapusiškai paaiškintų atsparumą. Visi egzistuojantys modeliai turi mažesnio ar didesnio laipsnio apribojimų.
- Atsparumas egzistuoja dėl aibės sąlygų – šios sąlygos gali lemti, ar atsparumo lygis yra aukštas – organizacija atspari, ar jis yra žemas – organizacija pažeidžiama. Toks

atsparumo spektras (dar kitaip, jį galima įvardinti – atsparumo gebėjimų branda) gali būti stebimas: skirtingose organizacijose, patiriančiose tą patį išbandymą; vienoje organizacijoje, patiriančioje skirtingus išbandymų tipus, arba vieną išbandymą, tačiau skirtingais laiko tarpsniais; patirianti vidinius išbandymus skirtingose organizacijos funkcijose. Atsparumo spektras svyruoja nuo reaktyvios būsenos, apimančios paprastas atsako formas į nenumatytus atvejus, link proaktyvaus pasirengimo, pasiekiant tokį lygmenį, kai organizacija tampa atsparesnė vis didesnio masto neapibrėžtumams.

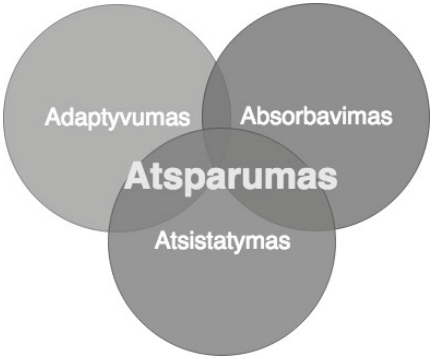
- Atsparumas yra formuojamas kai yra geras rizikų valdymo pagrindas. Retai kuri organizacija yra atspari atsitiktinai. Jų požiūris formuojant atsparumą dažniausiai bus pagrįstas trimis esminiais rizikų valdymo faktoriais: tinkamo rizikų įvertinimo, stebėsenos bei tinkamos komunikacijos apie jas.

Bendrinėje kalboje atsparumas apibrėžiamas kaip gebėjimas atgauti originalią formą ar poziciją po sulenkimo suspaudimo, ar tempimo. Taigi kalbant apie sistemas atsparias atakoms, pabrėžiamas jų gebėjimas atsistatyti po atakos, kas yra spaudimo ar tempimo analogas, arba bent išlaikyti autonomiško atsistatymo potencialą. Bishop ir kt. (2011) pažymi, kad šios savybės reiškia tai, kad sistema neturi nustoti visiškai funkcionavusi; ji turi iki tam tikro laipsnio išgyventi tam, kad būtų išlaikomi gebėjimai atsistatyti autonomiškai. Tad kibernetiniame domene, atspari sistema vykdo esmines savo funkcijas net paveikta potencialių grėsmių ar trikdant jos veiklą. Šios atsparumo idėjos įtvirtintos ne tik teoriniuose modeliuose, jas savo veikloje bandė diegti ir organizacijos, ieškančios būdų, kaip padidinti tam tikrų sistemų atsparumą nepalankiems reiškiniams. Taip JT Tarpvyriausybinė klimato kaitos komisija apibrėžia atsparumą kaip sistemos ir jos komponentų gebėjimą numatyti, absorbuoti, prisitaikyti ir atsistatyti nuo pavojingo įvykio laiku ir efektyviai, kartu su savo esminių bazinių struktūrų ir funkcijų išsaugojimu, atstatymu ir patobulinimu (IPCC, 2012).

Vienas vėlyvesnių atsparumo konceptų suformuotas Sansavini ir Nan (2017), kurių manymu, tolimesnė atsparumo terminijos plėtra turėtų apimti ir endogeninius (vidinius), ko gero, dažniausiai kontroliuojamus ir egzogeninius (išorinius nekontroliuojamus) veiksnius bei atsistatymo pastangas. Pagal Sansavini ir Nan (2017) apibrėžimą, atsparumas gali būti suvokiamas kaip aibė gebėjimų, kuriuos plėtojant didinamas ir sistemos atsparumas:

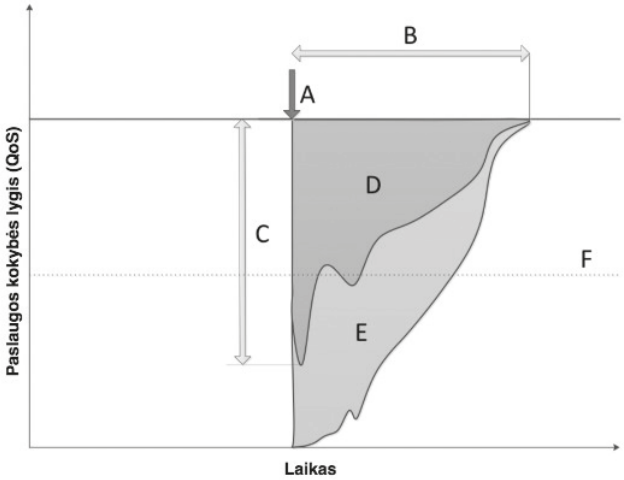
- Absorbavimo (angl. *absorbtive*) gebėjimai – sistemos gebėjimai atlaikyti pokyčius ar griaunančius įvykius, sumažinant pradines neigiamas pasekmes. Sansavini ir Nan (2017) šio gebėjimo matavimui siūlo taikyti tvirtumo matą, kuris Bruneau ir kt. (2003) apibrėžiamas kaip sistemos galia atsilaikyti prieš sutrikdymus. Taigi, šiame kontekste, pagal Bruneau ir kt. (2003), Gao ir kt. (2011) bei Sansavini ir Nan (2017), atsparumas turėtų būti suvokiamas kaip sistemos gebėjimas atsilaikyti prieš griaunančias jėgas ir sumažinti sistemos veiklos nukrypimus. Šis tvirtumu paremtas absorbavimo gebėjimas gali būti plėtojamas dubliuojant sistemos komponentus (angl. *system redundancy*) ar funkcijas – inžinerijoje tai įgyvendinama diegiant atsargines kopijas, t.y. padarant sistemą saugesne žlugti.
- Adaptyvimosi (angl. *adaptive*) gebėjimai – endogeniniai sistemos gebėjimai adaptuotis prie pokyčių ar griaunančių įvykių siekiant sumažinti griaunamas pasekmes. Šis gebėjimas plėtojamas per saviorganizaciją (Sansavini ir Nan, 2017).

- Atsistatymo gebėjimai – sistemos gebėjimai atsistatyti po pokyčių ar griaunančių įvykių. Pagal patį paprasčiausią suvokimą, tai yra sistemos gebėjimas būti pataisytai. Ši savybė yra ypač aktuali kritinės infrastruktūros sistemose (žr. 7 pav.).



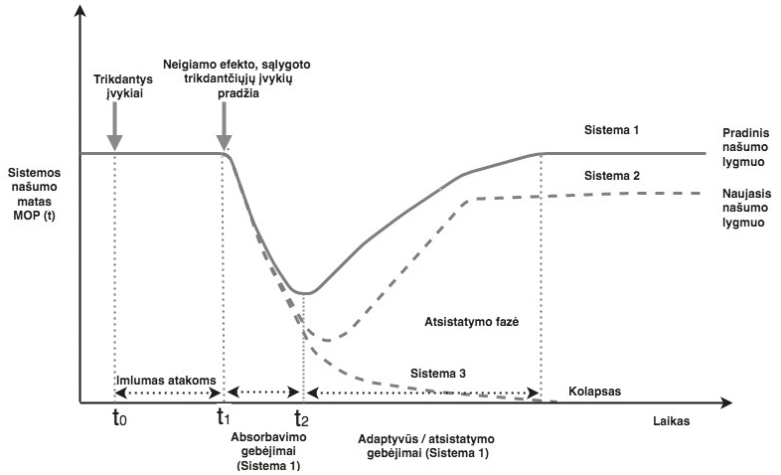
Šaltinis: *parengta autoriaus, pagal* Sansavini ir Nan, 2017
7 pav. *Atsparumo konstrukciniai komponentai*

Sistemos atsparumą vaizduojant grafiškai, Bishop ir kt. (2011) išskiria tokias dedamąsias (žr. 8 pav.): A ir B atvaizduoja laiką, kuris reikalingas sistemai grįžti į savo veikimo pusiausvyrą (angl. *equilibrium*); C atvaizduoja maksimalų sistemos sutrikdymą; alternatyvus atsakas į sutrikdymą žymimas E; F žymi ribą, kurią peržengus paslaugų kokybės kontekste sistemos veikimas pasiekia pavojingą lygmenį; X – ašies pagalba atvaizduojamas bendras sistemos laikas; Y – paslaugos kokybės lygis (en. *quality of service - QoS*).



Šaltinis: *Bishop ir kt. (2011)*
8 pav. *Pagrindiniai atsparumo proceso komponentai*

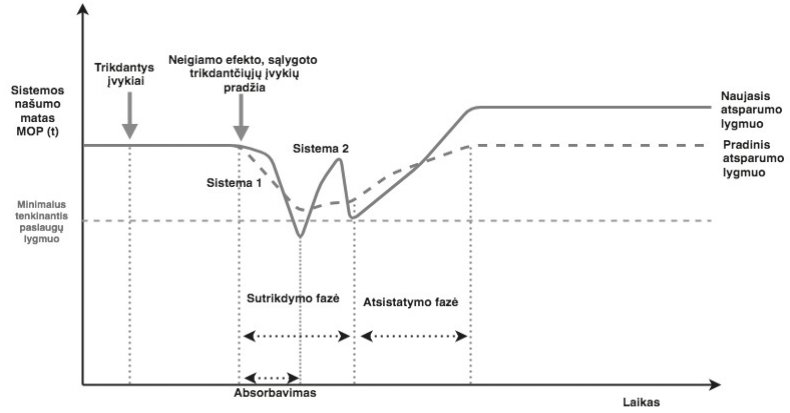
Pagal Nan ir Sansavini (2017), sistema Nr. 1 sugrįžta į savo pastoviąją būseną po atsistatymo iš žemiausio sutrikdymo lygmens. Sistemos Nr. 2 našumas pasiekia naują pastovųjį lygį, kuris yra mažesnis nei pradinis. Sistemos Nr. 3 našumo lygis nukrenta ženkliai ir galiausiai sistema žlunga – tai sąlygoja nulinį jos našumą (žr. 9 pav.). Pirmosios dvi sistemos lenkia trečiąją trimis atsparumo rodikliais: imlumu atakoms, absorbavimo bei adaptyvaus atsistatymo gebėjimais, tad, yra atsparesnės už trečiąją sistemą. Tyrėjai pastebi, kad galimas scenarijus yra toks: kai kurios sistemos yra tvirtesnės trikdančiųjų įvykių atžvilgiu, pavyzdžiui, sistemos Nr. 1 našumo lygis nukrenta mažiau nei sistemos Nr. 2, tačiau sistemos Nr. 1 atsistatymas iki pradinio našumo lygio užtrunka ilgiau, todėl tiesaus atsakymo į klausimą, kuri sistema yra labiau adaptyvi ir lengviau atsistatanti, nėra.



Šaltinis: *Nan ir Sansavini (2017)*

9 pav. *Esminiai sistemos atsparumo gebėjimai*

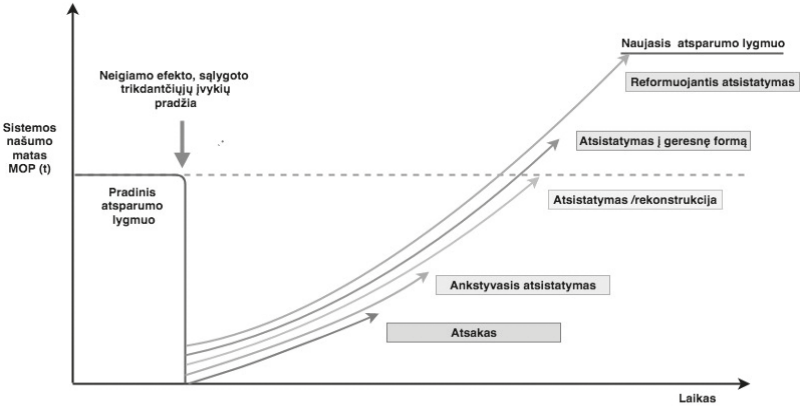
Kai sistema atsistatymo metu yra modifikuojama, naujasis našumo lygmuo gali būti ir didesnis už pradinį (Nan, Sansavini, 2017). Be to, autoriaus nuomone, kiekvienos sistemos siekiamybė turėtų būti kuo labiau sumažinti sutrikdymo ir atsistatymo fazių laiką. Taip pat pažymėtina, kad tinkamas sistemos pasirengimas neigiamų trikdančiųjų įvykių daromam poveikiui sąlygoja jos gebėjimą išlaikyti našumo lygį aukščiau virš suvokiamo minimalaus tenkinančio paslaugų ribos, kaip yra sistemos Nr. 1 atveju, arba, jei minimalus tenkinantis paslaugų lygmuo nukrenta, buvimas nepageidaujamoje būsenoje gali būti trumpesnis.



Šaltinis: *parengta autoriaus*

10 pav. *Krizėms pasirengusios sistemos atsparumo gebėjimai*

Taip pat vertėtų išskirti ir Lallemant (2013) modelį, pagal kurį, atsistatymas turėtų vykti į geresnę būseną nei buvo prieš tai, nes jei prieš tai buvusi sistemos būsena, paveikta neigiamo įvykio, sąlygojo sisteminį žlugimą, reiškia, kad ji nebuvo tobula. Po žlugimo, išmokstamos tam tikros pamokos, pašalinami sistemų pažeidžiamumai, geriau pasirengiama potencialioms panašaus pobūdžio atakoms.



Šaltinis: *Lallemant (2013)*

11 pav. *Sistemos atsistatymo į geresnę būseną gebėjimai*

Lallemant (2013) taip pat skiria kelias atsistatymo fazes. Pažymėtina, kad modelis formuotas pagal katastrofų kontekstą, todėl jame sutinkamos tokios formuluotės kaip žmogiškos aukos ir sužalojimai, kurie ne visuomet būdingi kibernetinių grėsmių sukeliamiems padariniams, tačiau svarstant kibernetines grėsmes gyvybiškai svarbioms sistemoms, galima būtų įžvelgti ryškesnes sąsajas tarp šių reiškinių.

- Atsakas – stabilizavimosi procesas, naujų aukų ar sužalojimu, galinčių kilti dėl katastrofos netikėtumo, prevencija.
- Ankstyvasis atsistatymas – šios fazės tikslas atsakyti į po krizinio laikotarpio ekstremalių pažeidžiamumų keliamas grėsmes: saugios prieglaudos nebuvimas, fizinės ar ekonominės saugos trūkumas.
- Atsistatymas (rekonstrukcija) – grįžimas į prieš krizinį buvusį – pradinį sistemos lygį.
- Atsistatymas į geresnę būseną – tas, kas atstatyta, turėtų būti atsparesniu.
- Reformuojantysis atsistatymas – sistemos kertinis reformavimas sukuriant kokybiškai naujas sistemos formas bei jose vykstančių procesų dinamiką.
- Atsparumo teorinė raida valdymo aspektu (Lallemant, 2013).

Atsparumo teorinė raida, prasidėjusi su anksčiau minėto Holling (1973) ekologinių sistemų studijomis, nagrinėjančiomis ekologinio atsparumo konceptus, vėliau imta naudoti socialiniuose moksluose, ilgainiui ėmė evoliucionuoti šiuose dviejuose visiškai skirtinguose epistemologinėse bendruomenėse, iš kurių autorius perėmė sistemų ontologiją. Manoma, kad atsparumo taikymo socialiniuose moksluose pagrindą sudarė kompleksiškumo (angl. *complexity*) teorijos atsiradimas. Ilgainiui atsiradęs kaip radikalus būdas galvoti apie pokyčius ir stabilumą, atsparumas, kaip ir darnumas, atlieką tarpdisciplininio, tam tikras konceptualias ribas nustatančio objekto funkciją (Brand ir Jax, 2007; Welsh, 2014). **Būdami teoriškai mobiliais** šie konceptai nuo pat jų atsiradimo 1970-aisiais taikyti įvairiuose domenuose evoliucionavo ir papildydami vienas kitą transformavosi į vientisą tyrimų metodiką, kuri ėmė įgauti vis labiau centrinį vaidmenį akademiniame ir politiniame diskurse, o ypač – neužtikrintumo ir rizikų valdymo srityse (Welsh, 2014). Šio amžiaus pradžioje, atsižvelgiant į įvairius žmonijai kylančius iššūkius įvairiose veiklos srityse, buvo stebimas gan didelis šių sričių atstovų susidomėjimas atsparumu, o tai lėmė nemažo skaičiaus apibrėžimų, procesų ir valdymo sistemų atsiradimą, kurie įnešė tam tikros painiavos į reiškinio konceptualizavimą (Gibson ir Tarrant, 2010). Papildomo sąmyšio kelia ir tai, kad atsparumo sąvokos taikymas neapsiriboja konkrečiu lygmeniu; jos taikymas vyksta: individualiame, bendruomeniniame (sociumo), organizaciniame, nacionaliniame, regioniniame lygmenyse ir įvairiose srityse: ekologijoje, psichologijoje, vadyboje, nenumatytų situacijų valdyme, IRT inžinerijos ir IRT saugumo srityse. Kaip pažymi Flynn (2011), tokia atsparumo terminijos gausa įvairiose disciplinose sukelia tam tikrą sąmyšį. Pažymėtina, kad atsparumo terminas, kuris pagal Welsh (2014) tam tikrame savo evoliucijos etape kaip atsparumo studijos, ėmė įgauti savitus bruožus ir tapo naudotinu įvairiose akademinėse disciplinose, politiniuose, privataus ir viešojo sektoriaus diskursuose. Taigi, būdamas plačiai taikomas ne tik teorinėje, bet ir praktinėje plotmėje, atsparumo požiūris vis labiau integruoja ne tik akademinius, bet ir viešojo valdymo diskursus, taip kiekvieną jų skatindamas įtakoti vienas kitą. Atsparumo konceptas sutinkamas net tokiose srityse kaip sveikatos apsauga, kur atsparumo formavimas ir gebėjimų atsispirti nuo nenumatytų situacijų ugdymas atskiruose sektoriuose gali būti matomas kaip nacionalinio sveikatos sektoriaus vienas iš kertinių elementų (Chandra ir kt., 2010). Pastangos koncentruoti tokį multifunkcinį, multidimensinį, sudėtingą konceptą į vieną objektą bei nuolatinis įvairių autorių bandymas egzistuojančias atsparumo idėjas modifikuoti ir bandyti pritaikyti naujomis aplinkybėmis sąlygoja

dar didesnį atsparumo, kaip tyrimų lauko, terminijos komplikuotumą (Gibson ir Tarrant, 2010). Nors egzistuoja nemažai modelių, apimančių bendruomenių atsparumo kontekste vykstančių resursų sąnglaudos ir jų efektyvaus valdymo klausimus, sunkumų kyla ir matuojant bendruomenių atsparumą siekiant suvokti šį procesą formuojančius sisteminius komponentus (Chandra ir kt., 2010). Sudėtingumas taip pat glūdi ir nustatant atsparaus valdymo subjektus ir objektus. Kaip pažymi Joseph (2013), prieš bet kokius valdymo bandymus yra būtina sukurti atitinkamą valdymo erdvę ir apibrėžti valdymo objektus arba subjektus. Kai kurie autoriai mato ir pozityvias tokių reiškinių puses. Kaip teigia Bourbeau (2013), nepaisant tokio plataus taikymo sąlygoto bendro konsenso dėl atsparumo apibrėžimo nebuvimo, susiformavo pagrindinės atsparumo kryptys: atsparumas inžinerijoje, ekologinis atsparumas, socio-ekologinis atsparumas. Taip pat gan ryškus organizacinio atsparumo teorinis laukas. Vertindamas šiuos procesus iš indėlio į teoriją perspektyvos, Flynn (2011), pažymi, kad pats faktas, jog įvairialypės tyrėjų, atstovaujančių skirtingas disciplinas, grupės rodo susidomėjimą atsparumo konceptu, padeda įvairiapusiškai geriau suvokti ir valdyti globalias ir socialines rizikas. Atsparumas suformuoja intelektualų pagrindą šioms diskusijoms, kuris sąlygoja naujų nagrinėjamo reiškinio pjūvių susiformavimą. Dabartinio atsparumo suvokimas, pagal Joseph (2013), kyla iš naujų ekologinio atsparumo ir žmonių prisitaikymo kompleksinėse didelėse sistemose konceptų interakcijos apmąstymo, akcentuojant tokius dalykus kaip kompleksiškumas, savi-organizacija, funkcinė įvairovė ir nelinijiniai elgsenos būdai (Joseph, 2013). Pažymėtinas minėto autoriaus pastebėjimas, pagal kurį, socialinių sistemų adaptyvumo gebėjimai priklauso nuo jų institucinės gebos absorbuoti sistemą šokiruojančius veiksnius, o krizės gali vaidinti konstruktyvų vaidmenį resursų valdymo kontekste, priversdamos organizacijas įvertinti mokymosi, adaptacijos ir atsinaujinimo aspektus (Joseph, 2013). Organizacinis atsparumas reikalauja planavimo gebėjimų, įgūdžių formavimo vykdant nuolatines pratybas, mokantis iš savo klaidų ir nagrinėjant gerąją praktiką integruojant naujus veikėjus ir specializuotas agentūras. Individai turi išsiugdyti lankstumo bei atsparumo gebėjimus. Lankstumo konceptas išpopuliarėjo anglakalbėje pasaulio dalyje ir ypač gerai atitiko globalaus neužtikrintumo būseną, pripildytą įvairių galimų iššūkių sistemai. Kartu tokiu požiūriu pripažįstamas sistemos vidinis sudėtingumas. Po 9/11 įvykių, atsparumas atitinka pasaulėžiūrą, orientuotą į globalias teroristines grėsmes, ekonominius iššūkius, natūralius (gamtinius) kataklizmus ir ekologines bei epidemines grėsmes (Joseph, 2013). Welsh (2014) vienas pagrindinių teiginių yra, kad mobilizuodamas sistemos metakonceptą bandant surasti sociogamtinius arba socioekonominius saitus, atsparumo teorijos materializuoja dvi abstrakcijas. Visų pirma, tai piliečių įtrauktis į praktikas, suteikiančias atsparumui prasmę ir buvimą. Antra, tai sistemą ištinkančių šokų natūralizavimas, konceptualiai juos išdėstant post-politinėje erdvėje, kur vienintelis ir neabejotinas tikrumas (angl. *certainty*) yra visiškas neapibrėžtumas (angl. *uncertainty*).

Bourbeau (2013) pažymi, kad nėra plačiai taikomų atsparumo modelių, o kaip atsparumas vertinamas priklauso nuo konkretaus konteksto ir perspektyvų. Atsparumas visuomet yra laipsniškas reiškinys, neegzistuoja visiško imuniteto šokams ir sutrikdymams. Visuomenės gali būti labiau ar mažiau atsparios tiek sinchroniškai, tiek diachroniškai. Atsparumas išgyvena nuolatinę kaitą (angl. *flux*). Tai nėra fiksuotas atributas ar nekintama

visuomenės ar individo charakteristika. Nei viena visuomenė nėra pastoviai atspari, išreikšta stabilumu ar variacijų nebuvimu. Kadangi atsparumo plėtojimo procesas niekada negali būti galutinai baigtas, atsparumas nereiškia baigtumo. Atsparumo procesas yra dinamiškas ir nuolatos judantis. Atsparumas yra visuomet normatyviai atviras, priklausomai nuo abiejų referentinių sistemų konceptualizacijos ir krizės ar šoko masto. Tam tikrais atvejais, kai atsparumas sąlygoja rigidiškas kolektyvinio ar nacionalinio identiteto struktūras, jis gali būti neigiamas, o kai sąlygoja pageidaujamą pokytį – teigiamas reiškinys. Taigi konceptas turi aibę savybių, kurios pagal nutylėjimą negali būti laikomos teigiamomis. Pagal Gitz ir Meybeck (2012), nagrinėjant sistemos atsparumą skirtinos kelios esminės perspektyvos. Visų pirma, tai – rizika – konceptas, taikomas galimam sistemų būsenų sukrėtimo potencialui įvertinti. Šiame kontekste, turėtų būti apimami tokie veiksniai, kaip tikimybės, poveikio (angl. *impact*) pasireiškimo tikimybės nežinomumas, sunkumas (angl. *severity*), ekonominis ir laiko mastai, tiesioginės ir netiesioginės išlaidos. Kitas svarbus elementas – pažeidžiamumas, kuris yra dinaminis, sudėtingas konceptas, apibrėžiantis sistemos polinkį patirti neigiamą poveikį. Konceptas egzistuoja laiko ir erdvės skalėse ir yra priklausomas nuo ekonominių, socialinių, geografinių, demografinių, kultūrinių, institucinių, valdysenos bei aplinkos faktorių. Pažeidžiamumo išmatavimui būtina atsižvelgti į įvairias dimensijas (IPCC, 2012; Gitz, Meybeck, 2012). Dviejų dimensijų sistemos adaptyvus gebėjimas: a) adaptuotis prie pokyčių; ir b) susidoroti su šokais ir juos absorbuoti, yra dar vienas dinaminis atsparumo gebėjimas, suformuotas aplinkos, socialinių, kultūrinių, politinių ir ekonominių galių, kurios nulemia sistemos pažeidžiamumą. Adaptyvumas atskleidžiamas visiems išvardintiems elementams darant poveikį per sistemos jautrias vietas vertinant sistemų ir jų vidinių komponentų reakciją į šokus Gitz ir Meybeck (2012).

1.5.1. Atsparumo formavimas: nacionalinio saugumo perspektyva

Kalbėdamas apie nacionalinio saugumo ir kritinės infrastruktūros apsaugos bei atsparumo sąsajų klausimus, vertėtų išskirti Fjader (2014) idėjas, kuris, pažymėdamas globalizacijos perspektyvą, kelia aibę klausimų apie tai, kaip galima būtų suformuoti atsparią naciją, kaip siejasi atsparumas ir nacionalinis saugumas, kuris yra viena esminių valstybės atsakomybių, ir kokią vertę jis galėtų sukurti. Taip pat Fjader (2014) pastebi, kad būtų pravartu atsakyti į klausimą, koks saugumo ir atsparumo tipas galėtų būti įgyvendinamas ir kokie jo būtų tikslai. Kaip pažymi Fjader (2014), vienas esminių klausimų formuojant nacionalines atsparumo strategines plėtros kryptis yra būtinybė apibrėžti, kaip atsparumas siejamas su valstybės atsakomybėmis valdyti nacionalinį saugumą. Taip pat kyla klausimai, ar atsparumas yra integruotas nacionalinio saugumo elementas, ar jis yra jo alternatyva ir jei taip – kokią pridėtinę vertę gali suteikti atsparumo plėtojimas, lyginant su nacionaliniu saugumu, kaip turėtų vykti šių dviejų reiškinių balansavimas juos užtikrinant. Kalbant ir mąstant saugumo, kaip strategijos, terminais, strateginio saugumo tikslas yra sustabdyti grėsmę prieš jam materializuojantis ar įvykstant jo eskalacijai arba, blogiausiu atveju, įveikti šią grėsmę kiek įmanoma greičiau ankstyvosiose jos stadijose. Kalbant apie saugumą iš erdvinės perspektyvos, dažniausiai tai reliatyviai specifiškas reiškinys, sukoncentruotas ties asmenimis, organizacijomis, infrastruktūromis ir teritoriniais vienetais. Jei šių saugumo

objektų saugumas yra sukompromituojamas arba saugumo objektas yra sunaikinamas, tai laikytina kaip saugumą įgyvendinančių subjektų ir pačios saugumo sistemos nesėkme. Saugumas iš savo tikslų perspektyvos yra gan specifinis reiškinys, o jo sėkmės laipsnis yra pakankamai išmatuojamas. Atsparumas, kita vertus, kombinuojant jį su proaktyviomis ir reaktyviomis priemonėmis, yra taikomas bandant sumažinti atsparumo objektui kylančių grėsmių poveikį, tačiau jo uždaviniai, savo esme, neapima prevencinių veiksmų ir net pagal atsparumo taikymo filosofiją, preventyvios priemonės, tikėtina, kad dėl pernelyg dinamiškos grėsmių prigimties niekada neduoda norimo efekto – taigi reikėtų susitelkti ties kritinėmis laikomų viešųjų paslaugų sutrikdymų mažinimu, kai tam tikra grėsmė jau yra įvykusi**. Šie teiginiai, iš esmės, apibrėžia idėjinę dviejų konceptų takoskyrą ir orientaciją: saugumo – į prevenciją, atsparumo – į sutrikdymų mažinimą.** Kaip pažymi Fjader (2014), atsparumas turi mažesnį erdvinį apibrėžtumą nei saugumas, ypač tai akivaizdu nagrinėjant atsparumą iš sudėtingų sistemų arba laike ir erdvėje paplitusių vertės grandžių perspektyvos. Atsparumas, priešingai nei saugumas, teigia gebėjimą adaptuotis prie sutrikdymų ir atsistatyti po jų į normalumo būseną per priimtiną laiko tarpą, tačiau, kaip pažymi Fjader (2014), nepaisant to, kad atsparumas ir saugumas turi skirtingas erdvines ir laikines savybes, abi savybės taikytinos naujose nacionalinių saugumo strategijų paradigmose. Tad pagrindinis diskusijos tikslas būtų atsakyti į klausimą, kaip jos viena su kita siejamos ir, kaip surasti tarp jų balansą saugumo formavimo tikslų bei optimalaus resursų panaudojimo perspektyvose. Šis, iš pirmo žvilgsnio lengvu atrodančio uždavinio sprendimas nėra jau toks akivaizdus. Kita vertus, saugumas ir tvirtumas bandant sumažinti grėsmės ir neigiamą poveikį turinčio įvykio tikimybę, tam tikra prasme, formuoja atsparumo pagrindą. Tai vyksta kartu su šių dviejų priemonių indėliu į esminių saugumo struktūrų ir resursų palaikymą (Fjader, 2014). Kitu atveju, atsparumas gali būti matomas kaip integruotas nacionalinio saugumo elementas, turintis specifinį tikslą pateikti priemonių rinkinį, galintį padėti atsakyti į nenumatytų ir netikėtų grėsmių keliamus iššūkius. Atsparumas taip pat gali būti veiksminga priemonė, kai iš finansinės perspektyvos nėra racionalu taikyti preventyvų požiūrį tų grėsmių atžvilgiu. Bet kokiu atveju, strateginis tikslas turėtų būti rizikos esminėms funkcijoms mažinimas ir priimtino apsaugos lygmens pasiekimas, tuo pat metu užtikrinant pagrindines visuomenės funkcijas bei jų atsistatymą racionaliais terminais, patiriant racionalias sąnaudas (Fjader, 2014).

1.5.2. Atsparumas kaip savybinis organizacijos konstruktas

Kaip pažymi Welsh (2014), egzistuoja dvi pagrindinės, tam tikra prasme, konverguojančios atsparumo teorijos formos, atsiradusios žmogaus protą ir kūną nagrinėjančiose disciplinose. Tai labiausiai pasireiškė psichologijoje bei gamtos ir visuomenės disciplinose – ekologijoje ir ekonomikoje. Nepaisant šios pradinės atsparumo idėjų specializacijos, atsparumo teorijos ir tyrimai yra stipriai orientuoti į tarpdisciplininės mokslines bendruomenes ir retai būna orientuotos vienos disciplinos problemoms spręsti, todėl idėjinė koncentracija dažnai vyksta ties jungtiniais konceptais, tokiais kaip asmenybė–visuomenė (psicho-socialinis atsparumas), bio-fizinė aplinka–visuomenė (socio-ekologinis atsparumas) (Welsh, 2014). Kibernetinio atsparumo tyrimų kontekste šį konceptą galima būtų

apibūdinti kaip kibernetinė aplinka–visuomenė. Be dviejų psicho-socialinio ir socio-ekologinio diskursų egzistuoja trečiasis – socialiniam subjektui kylančių rizikų ir grėsmių valdymo, kuris persidengia su minėtais dviem diskursais, tačiau teoriškai susigretina ir su politiniu, visuomeniniu atsparumo ir tvirtumo konceptais, saugumo, katastrofų valdymo ir tarptautinės plėtros kontekstuose, kuriuose atsparumo terminas tapo politiškai priimtinu pasirinktu terminu (Welsh, 2014). Ne išimtis ir organizacinis domenas bei jo atsparumas, kurį McManus (2008) apibūdino kaip „organizacijos funkcija veikianti kompleksiškose, dinaminėse ir susijungusiose aplinkose, apimanti situacijos žinomumą, esminių pažeidžiamumų valdymą, adaptyvius gebėjimus". Kadangi organizacijos yra integrali kiekvienos bendruomenės dalis, neretai bendruomenių atsparumas yra tarpusavyje sietini reiškiniai, o tokios sąsajos rezultatas yra kritinės svarbos organizaciniam atsparumui suteikimas. Kalbėdami apie bendruomenių ir organizacinio atsparumo sąsajas, šiuos reiškinius nagrinėjantys tyrėjai pažymi, kad organizacinis atsparumas, būdamas kertiniu elementu, padedančiu bendruomenėms turėti gebėjimus planuoti, pasirengti ir atsakyti į iššūkius krizių atvejais, gali būti ir organizacinio konkurencingumo ir bendros adaptyvios kultūros ugdymo pagrindu (Seville, Vargo, Lee, 2013). Atkreipdami dėmesį į tai, kad norėdamos būti atspariomis organizacijos turi būti vedamos tvirtos lyderystės, suvokti savo operacijų aplinką ir turėti gebėjimus adaptuotis prie pokyčių, Seville, Vargo ir Lee (2013) brėžia paraleles tarp atsparumo ir konkurencingumo, nes, autorių nuomone, būtent šie atsparumą sąlygojantys faktoriai nulemia ir organizacijos gebėjimą konkuruoti savo sektoriuje bei adaptuotis prie jame esančių iššūkių. Sąsajos tarp atsparumo ir konkurencingumo išreiškiamos ir per jos gebėjimą suvokti situaciją (angl. *situational awareness*) ar gebėjimą interpretuoti veiklos informaciją bei suprasti, kokią reikšmę ši informacija turi šiuo metu ir ateityje – būtent šis gebėjimas, anot Seville, Vargo ir Lee (2013), yra analogiškas konkurencinės aplinkos žinojimui. Atsparumas yra organizacijų multidimensinis, socio-techninis fenomenas, kuris apibrėžia kaip žmonės, individai ar grupės, valdo neužtikrintumą. Kaip teigia Seville et ir kt. (2013), cituodami skirtingus autorius, organizacijos į neužtikrintumą atsako įvairiais būdais – tai gali apimti vidinės kontrolės mechanizmų centralizavimą (Pfeffer, 1978 iš Seville ir kt., 2013), jos mokosi (Christianson ir kt., 2009;), gerina savo kūrybinius gebėjimus (Kendra, Wachtendorf 2003), adaptuojasi (Vogus, Sutcliffe, 2007). Atsparumo literatūroje pastebima, kad nepaisant to, jog dauguma organizacijų lyderių pripažįsta poreikį didinti organizacijų atsparumą, kalbant apie atsparumo teikiamas naudas, organizacijoms sudėtinga rasti sąsajų tarp gebėjimų atsakyti į krizes ir operacijų efektyvumo bei prioritetizuoti atsparumo veiklas lyginant su kitais organizacijos procesais, taigi ir skirti reikiamų lėšų atsparumo plėtojimui. Organizacijoms siekiant investuoti į atsparumą, būtina taikyti platesnį požiūrį nei tiesiog draudimą nuo nenumatytų situacijų, – šios investicijos turėtų prilygti skiriamoms naujai įrangai ar žmogiškų resursų reikmėms (Vargo ir Stephenson 2010).

Kalbėdami apie atsparios organizacijos apimamus gebėjimus, autoriai išskiria:

- „atšokimą atgal" (angl. *bounce back*) (Hale, Heijer 2006);
- tvirtumą (Tierney, 2003);
- absorbavimą (Berkes, 2007);
- išgyvenimą ir klestėjimą (Seville, 2009);

- adaptaciją (Dekker ir kt., 2008);
- gebėjimą atsakyti į įvairius sutrikdymus (Dekker ir kt., 2008);
- reguliarias ir nereguliarias grėsmes (Dekker ir kt., 2008);
- gebėjimą lanksčiai stebėti kas vyksta (Dekker ir kt., 2008);
- gebėjimą numatyti sutrikdymus (Dekker ir kt., 2008);
- gebėjimą mokytis iš patirties (Dekker ir kt., 2008).

Seville ir kt. (2008) apibūdina organizacijos atsparumą kaip jos gebėjimą kriziniu metu išgyventi ir net klestėti. Organizacinio atsparumo literatūroje diskutuojant apie organizacijos gebėjimą adaptuotis, šie du reiškiniai yra dažnai sugretinami ir klausiama, ar galima tarp jų dėti lygybės ženklą, t.y. ar adaptacija yra atsparumas (Lee ir kt., 2013), tačiau kai kurių autorių nuomone, atsparumas yra daugiau nei gebėjimas adaptuotis (Dekker ir kt., 2008). Vertinant iš kibernetinio saugumo perspektyvų organizacinis elementas yra ypač svarbus. Atsižvelgiant į tai, kad galutiniai organizacijoje naudojamų technologijų vartotojai dažnai neturi reikiamo su jų kasdienės veiklos metu vykdomomis funkcijomis susijusių rizikų suvokimo. Taip pat pažymėtina, kad dauguma darbuotojų turi nedidelį technologijų suvokimo mastą, nepaisant to, kad naudojasi kompiuterinėmis darbo vietomis kasdieninėms užduotims spręsti, todėl tokio suvokimo formavimas kelia nemažą iššūkį. Neretai grėsmės yra apipintos sudėtingais techniniais aspektais, todėl efektyvaus saugumo įgyvendinimas turi būti lydimas tinkamo techninių ir procedūrinių apsaugos mechanizmų balanso. Nagrinėdami būdus, taikomus konceptualizuoti, suprasti ir įgyvendinti organizacinį atsparumą, Gibson, Tarrant (2011) išskyrė kelis esminius požiūrius, kuriuos jie sugrupavo į loginius–konceptualius modelius:

- Integruoti funkciniai atsparumo modeliai – atsparumas integruojamas į jau egzistuojančius teorinius instrumentus: veiklos tęstinumo ar nenumatytų situacijų, rizikų bei kokybės valdymą.
- Atribuciniai atsparumo modeliai – atsparumas bandomas paaiškinti iš didelį atsparumą turinčių organizacijų perspektyvos. Toks požiūris padeda atskleisti kokie organizaciniai atributai gali padėti organizacijai atsakyti į nežinomybės ir nenumatytų situacijų keliamus iššūkius.
- Kompoziciniai atsparumo modeliai – modelio pagrindą sudaro orientacija į strategijas ir politikas, formuojančias operacijų dualumą (angl. *duality*), gebėjimus operuoti ir rutininėse ir nerutininėse aplinkose.
- Eglės šablono (angl. *herringbone*) atsparumo modelis – bandomi apjungti keliuose modeliuose esantys atsparumo konceptai, taip užpildant kiekviename jų egzistuojančias spragas. Taikant šį modelį, pripažįstama, kad pagal nutylėjimą, dauguma organizacijų pastaraisiais laikais jau turi reikšmingus gebėjimus ir imasi aibės veiksmų, galinčių pagerinti atsparumo lygį.
- Atsparumo trikampio modelis – jį sudaro į tris kategorijas konceptualiai paskirstyti komponentai: procesiniai, resursiniai ir infrastruktūriniai gebėjimai bei lyderystės, žmogiškųjų resursų, žinių gebėjimai (Gibson, Tarrant, 2011). Išsami Gibson, Tarrant (2011) organizacinių modelių analizė pateikiama priede Nr. 2.

Atsparumą nagrinėjančioje literatūroje tam tikra dalis skiriama ir diskusijoms apie atsparumo matavimą. Kalbėdami apie organizacijos atsparumo matavimo poreikį Seville ir

kt. (2013) teigė, kad šio reiškinio išmatavimas gali pasitarnauti keturiems esminiams organizacijos poreikiams:

- Parodyti atsparumo plėtros progresą;
- Nustatyti atsparumo indikatorius;
- Susieti organizacijos atsparumo tobulėjimą su konkurencingumu;
- Pademonstruoti pagrindą su atsparumu susijusioms investicijoms pagrįsti.

Pagal autorius, atsparumas susitelkia ties socialiniais ir kultūriniais faktoriais organizacijoje, kuriuos ganėtinai sudėtinga išmatuoti ir susieti su finansiniais rezultatais, pavyzdžiui, nenumatytų situacijų pratybos ir jų efektas organizacijos atsparumui (Seville ir kt., 2013). Gibson ir Tarrant (2010) pažymi, kad dauguma egzistuojančių organizacinio atsparumo matavimo požiūrių klaidingai sukoncentruoti ties organizacinių atributų matavimu rutininėse aplinkose tikintis, kad šie atributai parodys tikrą atsparumo būseną. Tačiau realiose situacijose, priklausomai nuo organizacijai gresiančių iššūkių, kiekvienas atributas potencialiai funkcionuos skirtingai bei turės skirtingą poveikį bendrai atsparumo sistemai. Kadangi atsparumas susiformuoja objektui sąveikaujant su jo aplinka, geriausiu atveju, dauguma egzistuojančių modelių matuoja organizacijos atsparumo gebėjimus. Organizacinis kontekstas gali turėti dvejopą poveikį: tiek skatinantį atsparumo gebėjimus, tiek mažinantį jų potencialą; kurioje kreivės vietoje bus pozicionuojami atsparumo gebėjimai, priklausys nuo to, kaip organizacija valdo jos veiklai kylančias rizikas.

1.5.3. Atsparumas: sudėtingų adaptyvių sistemų perspektyva

Siekiant geriau suvokti atsparumą, konceptualiai yra pravartu taikyti sisteminę perspektyvą, kuri yra būdinga ir ankstesniuose poskyriuose minėtoms Holling (1973) ekologinio atsparumo teorijoms, ir 1990-aisiais tokių organizacijų kaip Atsparumo aljanso tinklas išplėtotoms iki žmogiškųjų, t.y. socioekologinių sistemų, idėjoms. Kai kurių autorių nuomone, atsparumas yra ypač taikytinas sudėtingų adaptyvių sistemų kontekste, kaip priemonė konceptualizuoti ir valdyti sistemose vykstančius pokyčius (Welsh, 2014). Sistemų atsparumas pačiu paprasčiausiu suvokimu yra sistemos gebėjimas vykdyti nustatytas funkcijas net tuo atveju, kai ji yra veikiama nenumatyto atvejo arba sutrikdymo ir tęsti operavimą, išlaikant tokią būseną, kuri galėtų būti laikytina normalia arba įprastine veikla (angl. *business as usual*). Pagal Hollnagel, Woods (2006), sistemos skirtingų komponentų atsparumas yra priklausomas nuo kitų sistemos komponentų atsparumo. Kalbant apie sistemos adaptacijos mechanizmus, pažymėtina, kad literatūroje, pagal Woods, Wreathall (2008) ir Vogus, Sutcliffe (2007), skiriami du adaptyvių gebėjimų tipai:

- adaptyvūs gebėjimai per veiklos tęstinumo ir rizikų valdymo veiklas, demonstruojami organizacijoms „atšokant“ (angl. *bounce banck*) išnaudojant iš anksto suformuotus planus ir gebėjimus;
- adaptyvūs gebėjimai susiformavę per nenumatytas situacijas, kurioms nebuvo pasirengta.

Kaip pažymi Fjader (2014), sistemų atsparumo suvokimą komplikuojantis reiškinys yra tas, kad yra sudėtinga rasti sistemą, kuri būtų visiškai izoliuota ir nepriklausytų nuo kitų kompleksiškų reiškinių, savo funkcijų vykdyme. Atsižvelgiant į tai, atsparumas

ir atsistatymas gali būti tam tikrų normalių būsenų aibė, individualiai apibrėžta kiekvienai sistemos vykdomai funkcijai. Taigi, alternatyvus požiūris į sistemos atsparumą būtų jos gebėjimo reaguoti į nepaprastas situacijas, ypač kai kalba eina apie sistemos gebėjimą absorbuoti sutrikdymus, išgyventi pokyčius ir išlaikyti tokį patį funkcinį, struktūrinį, identiteto ir grįžtamųjų ryšių lygį. Atsparumas kompleksiškose, adaptyviose struktūrose, tokiose kaip eko ir socialinės sistemos, yra suvokiamas kaip gebėjimas atsistatyti, reorganizuotis veikiamai šoko ar krizės ir šiems reiškiniams priešintis. Taigi, pagal Fjader (2014), atsparumo esmė yra adaptyvumas, kuris įgalinamas nelinijinės sisteminių elementų ryšių natūros. Atsižvelgiant į šiuos argumentus, galima daryti išvadą, kad sudėtingų adaptyvių sistemų kontekste, funkcionavimo normalumo suvokimas yra gebėjimas adaptuotis prie naujų veiklos sąlygų, susitelkiant ties esminių sistemos funkcijų išlaikymo, net tais atvejais, kai sistemos struktūra pakinta, ar laikui bėgant sistema sužlugdoma. Kalbėdami apie sistemos adaptyvumą, Gibson ir Tarrant (2010) pažymi, kad dažnai pamirštama, kad atsparumas nėra vien tik sistemos atsistatymas po nelaimės, tačiau tai turėtų būti sietina labiau su adaptyviais sistemos gebėjimais bei požiūriu, kaip organizacinė sistema supranta ir reaguoja į neapibrėžtumus išorinėse ir vidinėse aplinkose. Atspari sistema sumažina nesėkmių tikimybes, jų pasekmes, negatyvius ekonominius ir socialinius efektus bei sutrumpina atsistatymo laiką (Tierney, Bruneau, 2007). Atsparumas gali būti matuojamas infrastruktūros sistemos, patyrusios katastrofinį įvykį funkcionalumu ir pagal laiką, kuris reikalingas sistemai sugrįžti į prieš katastrofinį lygmenį (Tierney ir Bruneau, 2007). Atsparumo literatūroje išskirtas sistemos pusiausvyros (angl. *equilibrium*) elementas, kuris, kaip pastebi (Bourbeau, 2013), būdingesnis atsparumo diskursui inžinerijos domene. Pusiausvyros konceptas jame naudojamas nustatyti sąlygas, siekiant identifikuoti, kiek sistema gali nukrypti nuo savo fiksuoto veikimo pusiausvyros ir, nepaisant to, į tą pusiausvyrą sugrįžti, kai tik sutrikdymas praeina. Ekologinių sistemų atveju, pusiausvyros idėjos atsisakoma, čia atsparumas matomas kaip sistemos gebėjimų patirti sutrikdymus ir, nepaisant to, toliau išlaikyti savo funkcijas ir kontrolės mechanizmus. Socio-ekologines sistemas nagrinėjantys tyrėjai pažymi, kad takoskyra tarp socialinių ir ekologinių sistemų yra dirbtinai suformuota, šios krypties tyrėjai mato atsparumą ne tik kaip gebėjimą išlaikyti sistemai sutrikdymų keliamus iššūkius, bet ir kaip galimybę identifikuoti naujas saviorganizacijos, rekombinacijos formas bei naujas sistemos funkcionavimo trajektorijas (Bourbeau, 2013). Nagrinėdamas sistemų atsparumo (angl. *resilience*) ir sistemų pasipriešinimo (angl. *resistance*) skirtumus, Tierney ir Bruneau (2007) pažymėjo, kad pasipriešinimo komponentas pabrėžia prieš-katastrofines sušvelninimo priemones, kurios pagerina sistemos struktūrų, infrastruktūros elementų ir institucinių gebėjimų visumą, padedančią sumažinti katastrofos sąlygojamus praradimus. Savo ruožtu, atsparumas atspindi fizinių ir žmogiškųjų sistemų pajėgumų reaguoti į ekstremalius įvykius ir po jų atsistatyti didinimą. Nagrinėdami sisteminio tvirtumo ir atsparumo santykį ir bandydami atsakyti į klausimą, kas yra sistemos atsparumas atakoms, Bishop ir kt. (2011) pastebėjo, kad nepaisant to, jog šie du reiškiniai yra skirtingi, jų terminai dažnai vartojami sinonimiškai, o tai tam tikrais atvejais gali būti gan pavojinga, ypač nagrinėjant šiuos reiškinius iš tarpdisciplininės perspektyvos. Tyrėjai pažymėjo, kad tinkamam šių dviejų reiškinių skirtumo suvokimui ir kiekvieno jų vaidmens nustatymui kompiuterijos sistemose ir infrastruktūrose būtina tinkamai apibrėžti jiems būdingus sisteminius

elementus, o tam reikia išskirti esminius kiekvieno jų požymius, nustatyti vieningus matavimo principus bei identifikuoti atsparioms ir tvirtoms sistemoms būdingus gebėjimus. Labai dažnai atsparumo, tvirtumo ir išgyvenamumo konceptai yra lengviau paaiškinami iš sistemos veikimo efektyvumo perspektyvų, kadangi tai iš dalies yra lengviau paaiškinami ir kontroliuojami reiškiniai nei tokios abstrakčios sąvokos kaip konfidencialumas. Tačiau kai sistemos veikimo efektyvumas turi būti balansuojamas su konfidencialumu ir vientisumo reikalavimais, atsparios sistemos konceptas tampa miglotu. Sistemos tvirtumas (angl. *robustness*) apibrėžiamas kaip savo konstitucija tvirtas, atsparus objektas. Nepaisant viso savo tvirtumo masto, visuomet išlieka rizika, kad sistema gali žlugti. Tačiau, esant mažam atsparumo laipsniui, sistemai po ardomų veiksmų prieš ją sudėtinga sugrįžti į dalinai sutrikdyto veikimo būseną. Taigi, tokia sistema dėl savo dominuojančio tvirtumo elemento arba atsilaiko prieš atakas arba visiškai nustoja veikti ir neveikimo būsenoje išlieka tol, kol įvyksta įsikišimas (Bishop ir kt., 2011).

Taip pat būtina išnagrinėti ir sistemos išgyvenamumo (angl. *survivability*) elementą, kuris bendrinėje kalboje apibrėžiamas kaip gebėjimas egzistuoti po tam tikro įvykio ar sąlygos egzistavimo pabaigos. Bishop ir kt. (2011) sistemos išgyvenamuma apibūdina kaip gebėjimą egzistuoti net esant ženkliai kokybiškai sumažėjusioms operacinėmis sąlygomis. Kaip pavyzdį tyrėjai pateikia internetą, kuriame esant dideliam atakų skaičiui, bendrasis funkcionalumas būna paveiktas, tačiau mažai tikėtina, kad jo operavimas galėtų būti visiškai nutrauktas. Bishop ir kt. pažymi, kad sistemos, negalinčios operuoti esant minimaliam ar žemesniam už jį paslaugų kokybės (angl. *quality of service QoS*) lygmeniui, techniškai turėtų būti laikomos kaip nepajėgusios išgyventi – tai ypač taikytina kritinėms sistemoms ir programinei įrangai. Sklandus paslaugos lygio sumažinimas (angl. *graceful degradation*), t.y. kompiuterizuotos sistemos ar tinklo gebėjimas išlaikyti ribotą funkcionalumą, net tuomet kai didelė dalis šios sistemos yra sunaikinta, tam, kad būtų išvengta katastrofiško sistemos žlugimo, Bishop ir kt. (2011) laikomas vienu iš išgyvenamumo sudedamųjų dalių. Pagal Bishop ir kt. (2011) atsparumas, tvirtumas ir išgyvenamumas yra skirtingi reiškiniai, o gilesnė analizė parodo, kad visi jie tarnauja skirtingiems sistemos apsaugos ir gerovės užtikrinimui. Visi šie reiškiniai sudaro pagrindą sistemos patikimumo konceptualizavimui. Patikimumas (angl. *reliability*) suprantamas kaip savybė, sąlygojanti pasitikėjimą sistema. Patikimumas laikytinas sistemos sėkmės matu, kuris apibrėžia kaip sistema atitinka apibrėžtas autoritetingas sistemos funkcionavimo specifikacijas (Randell ir kt., 1978; Bishop ir kt., 2011). Pagal Welsh (2014), pastaruoju metu, ėmė rastis vis daugiau adaptyvių ir lanksčių atsparumo sistemų versijų, kurių idėjos akcentuoja, kad sistemos trapumas (angl. *brittleness*) kyla iš jos rigidiškumo ir centralizuotų valdymo ir kontrolės (angl. *command and control*) sistemų. Toks požiūris ypač stiprėja bendruomenių, klimato, plėtros ir žmonių saugos srityse. Pagal tokį požiūrį (išdėstytas *Demos ekspertų grupės* (angl. *think tank*) pranešime „Resilient Nation“), naujosios kartos atsparumas priklauso nuo piliečių ir bendruomenių, o ne nuo institucijų ar valstybės (Demos, 2010). Kaip pažymi Carpenter ir kt. (2001), atsparumas turi būti suvokiamas specifiniame kontekste atsakant į klausimą „Kokie? Kam?“. Tai reiškia, kad būtina apibrėžti, kokie sistemos elementai ar funkcijos yra atsparios ir kokiems pokyčiams. Jei sistema yra suformuota iš skirtingus lygmenis sudarančių elementų, ji gali būti atspari tam tikruose lygmenyse, tačiau nebūtinai kituose.

Tad natūraliai kyla klausimas, kaip valstybė ar organizacija gali būti atspari, jei aibė visuomeninių sistemų žlunga. Kita vertus, valstybė gali žlugti dėl didelių apimčių politinės ar ekonominės krizės net tuomet, kai dauguma jos sistemų yra nepaveiktos (Dahlman, 2011).

Atsparumas turi savo kainą, kuri yra kitokia nei bandant padidinti sistemos našumą. Kaip ir bet kokio resursų diversifikavimo atveju, egzistuoja praradimai ir sinergijos tarp produkcijos ir atsparumo bet kokioje socialinėje, ekonominėje, politinėje sistemoje. Finansinis sistemų atsparumo aspektas yra sunkiai įvertinamas, kadangi niekam nėra mokama už tai, kad sutvarko problemas, kurių dar nėra atsitikę, organizacijos dažniausiai nekreipia pakankamai dėmesio į sistemų atsparumo būklės pagerinimą (Dahlman, 2011). Tai taip pat tinkama argumentacija sociopolitinėse sistemose, kur atsparumo formavimas yra sutelktas į sistemos elgseną labiau nei į tikimasi rezultatą, todėl tiesmukai taikant atsparumo konceptus, tai gali sukelti problemas su socialinės sanglaudos veiksmais, sveikatos apsauga bei sociumo plėtra (Dahlman, 2011).

1.5.4. Atsparumas: politinė ir valdymo perspektyvos

Skirtingų sričių kiekis, kuriose taikant atsparumu grįstą požiūrį vienokiu ar kitokiu mastu struktūriškai įtakojamos valdžios politikos ar praktikos, apimtys nuolatos didėja. Tarptautiniame valdymo kontekste, pradedant ES institucijomis, baigiant JT organizacija, atsparumo taikymas labiausiai matomas tarptautinės plėtros, nenumatytų situacijų planavimo ir klimato kaitos bei darnios plėtros domenuose. Kaip pažymėjo Bourbeau (2013), atsparumo konceptai yra pakankamai menkai išplėtoti tarptautinių santykių ir politikos studijose ir tik pastaruoju metu stebimas tam tikras tyrėjų aktyvumas nagrinėjant šią sritį. Kita vertus, už akademinio diskurso ribų atsparumas ganėtinai greitai tapo plačiai paplitusia globalios valdysenos idioma (Walker ir Cooper 2011), kurioje jis veikia veikiau nei ideologija, skatinanti post-politines gyvavimo formas, orientuotas į nuolatinį prisitaikymą bei ilgalaikių lūkesčių atsisakymą (Duffield, 2011). Kaip pastebi Brasset ir kt. (2013), daugėja tvirtinančių, kad atsparumas yra daugiau nei tuščia metafora, o jos įtraukimas į šiuolaikinį politikos diskursą atskleidžia naujus valdymo metodų kaitos aspektus ir fundamentinį mąstymo poslinkį nuo senųjų šaltojo karo laikmečio saugumo logikų. Tyrėjai pažymi, kad su augančia rizikų tyrimų banga, kai bandoma ieškoti būdų gyventi su globaliomis nežinomybėmis (angl. *uncertainties*) nei joms priešintis, tarptautinių santykių ir politikos studijose susidomėjimas atsparumu sparčiai auga. Kalbėdamas apie atsparumo pozicionavimą visoje valdymo sistemoje, Fjader (2014), nagrinėdamas Australijos, Naujosios Zelandijos, JAV, Kanados, JK ir Nyderlandų saugumo strategijas, pastebi, kad nepaisant to, jog dauguma nagrinėtų valstybių savo saugumo strategijose akcentuoja atsparumą, atsižvelgiant į tai, kad jis siejamas su nacionaliniu saugumu, civiline sauga ir ekstremalių situacijų valdymu ir kritinės infrastruktūros apsauga, nėra vieningo šio reiškinio apibrėžimo. Pagal Fjader (2014), valstybių, t.y. nacionalinio saugumo užtikrinimo, kontekste, atsparumas yra gebėjimas atlaikyti netikėtus šokus ir atsistatyti arba tiesiog nuo jų „atšokti“ (angl. *bounce back*). Kaip pažymi Brasset ir kt. (2013), atsparumas tampa centriniu organizuojančiu principu šiuolaikinėje politinėje dienotvarkėje, tad atsparumo konceptas yra matomas kaip priemonė bandant atsakyti į aibę įvairių ir dažnai tarpusavyje nesusijusių

globalių (potvyniai, kibernetinis terorizmas, finansinės krizės, kritinės infrastruktūros sutrikimai ir pan.) neapibrėžtumų keliamus iššūkius bei bandant šiuos neapibrėžtumus geriau suvokti. Kalbėdami apie valdymo ir atsparumo sąsajas, Walker ir Cooper (2011) atsparumą mato išankstinėmis prognozėmis (angl. *anticipatory*) paremtu valdymu; Dean (2012), Joseph (2013), Reid (2012) atsparumą laiko neoliberalia valdymo forma. Pagal Reid (2012), būtent bandymai kultivuoti adaptyvius, savisaugą užsitikrinančius, už savo rizikų valdymą atsakingus subjektus sąlygoja neoliberalių valdymo modelių susiformavimą. Kaip pastebi Duffield (2012) ekstremalių situacijų planavimas XX a. pabaigoje apėmė įvykių prognozavimą, žinomų grėsmių išskyrimą bei visuomenės apsaugą taikant karines ir kvazi-karines priemones. Kovai su žinomais pavojais ir priešais buvo taikytas centralizuotas ir koordinuojamas reagavimas, kuris buvo organizuojamas per hierarchines valdymo ir kontrolės grandis. Toks pasirengimas ekstremalioms situacijoms yra priešingas paremtam atsparumo požiūriu, kai visuomenė mokoma naujų pasirengimo įgūdžių ir pasirengimo, adaptacijos bei gyvenimo su galimomis nepažintomis grėsmėmis įgūdžių (Brasset ir kt., 2013). Tokiame kontekste atsparumas laikytinas didesnių socioekonominių pokyčių atributu, sąlygojančiu poslinkį nuo liberalizmo link neoliberalizmo, kuriame vis dažniau taikomas; modernioms neoliberalistinėms sistemoms būdingas atsparumo, kaip adaptacijos, požiūris (Walker ir Cooper, 2011; O'Malley, 2010; Brasset ir kt., 2013). Nors politikos bei tarptautinių santykių srityje atsparumas nagrinėjamas pakankamai nesenai, jau pažymimas teorinių debatų painumas. Brasset ir kt. (2013) pastebi, kad atsparumo diskurse egzistuoja tam tikras neaiškumas tarp tokių konceptų kaip pasirengimas (angl. *preparing for*), „atšokimas atgal" (angl. *bounce back*) nuo įvykio, adaptacija (angl. *adapting to*) ir gyvenimas su (angl. *living with*) tarpusavio sąsajų, dažniau pagal nutylėjimą laikant, kad šie konceptai papildo vienas kitą, o ne vienas kitam prieštarauja. Nors, kaip pažymi Brasset ir kt. (2013), psichologinis „gyvenimo su" nežinomybe konceptas gan sunkiai suderinamas su bendriniu pasirengimo kultūros formavimu. Pagal autorius, atsparumo politika turėtų būti matoma kaip nenutrūkstanti interakcija tarp skirtingų veikėjų ir jų logikų ir apimti aibę klausimų:

- Kurie veikėjai ir ekspertinės žinios yra įtraukti į atsparumo gerinimo politiką ir praktiką?
- Kas gauna naudą iš atsparumo formavimo ir kas yra atskiriamas?
- Kur atsparumas susiduria su savo ribomis ir nustoja veikti (angl. *Break down*)?
- Kaip atsparumas gali būti pasipriešinimo (angl. *Resistance*) subjektu?
- Kaip atsparumo dienotvarkė galėtų būti formuojama (angl. *Occupied*) kitokiais būdais, galinčiais padėti apgalvoti problemą, pavyzdžiui, per tradiciją ar emociją?

Atsparumas dažnai vertinamas neoliberaliame valdysenos diskurse, kur atsakomybė už rizikas perkeliama nuo valstybės ant individų ir institucijų. Atsižvelgiant į šiuos argumentus, Welsh (2014) pastebi, kad galima stebėti valdysenos sistemų (angl. *governmentality*) plėtotę krypstant per atsparumą valdymo link. Kalbant apie atsparumo indėlį politikos mokslų domenui, pažymėtina, kad šiame kontekste vykdomas atsparumo nagrinėjimas per rizikų valdymo prizmę pagilina saugumizacijos teorijos išskiriamo referentinio saugumo objekto suvokimą ir praplečia šios srities diskursą klausimais, apimančiais pradedant finansinėmis architektūromis, baigiant tinklais ir kritine infrastruktūra (Lakoff, Collier, 2010; Lundborg,

Vaughan-Williams, 2011; Brassett, Holmes, 2013). Pasak Brasset ir kitų (2013), kaip ir globalizacijos konceptas, kurio populiarumas ėmė augti praėjusio amžiaus pabaigoje, atsparumo suvokimas turi tam tikrą produktyvų neapibrėžtumą ir leidžia skirtingo valdymo lygmens domenų interakciją. Nepaisant to, kad atsparumas dar tik besiformuojantis reiškinys, politiniuose dokumentuose ir praktikoje vis dar egzistuoja bendro šio reiškinio suvokimo trūkumas. Politiniai atsparumo aspektai gali būti suvokiami priklausomai nuo to, kaip konceptas naudojamas skirtinguose kontekstuose, laikotarpiuose bei prasmėse. Be to, nepakanka empiriškai pagrįstų akademinių įžvalgų, galinčių padėti nustatyti atsparumo taikymo organizaciniame domene mastą, būtina suvokti kaip atsparumo konceptai turėtų būti taikomi socialinėse sistemose (Brasset ir kt., 2013). Bourbeau (2013), plėtodamas Kopenhagos saugumo studijų mokyklos idėjas, išskiria resilientizmo (angl. *resiliencism*) sąvoką. Pagal autorių, iš esmės, resilientizmas, išryškindamas reikšmingus saugumizacijos sistemos elementus, galėtų sąlygoti naujus teorinius ir empirinius šiuolaikinio saugumo domeno suvokimo būdus ir padėti geriau suvokti saugumizacijos procesus, t.y. pagerinti saugumo problemų integravimą į egzistuojančius saugumo modelius, nagrinėjančius policinę funkciją ir gynybą. Resilientizmas turi didelį potencialą įnešti naujumo į saugumo ir valdymo sričių domenus. Resilientizmas praplečia atsparumo apibrėžimą už jo tradicinio suvokimo ribų, t.y. tokių, kuriose jis suvokiamas kaip aibė atsparumo objekto turimų savybių arba kaip pozityvios adaptacijos procesas kylančių grėsmių akivaizdoje. Fjader (2014), nagrinėdamas valstybės vaidmens evoliuciją teikiant politines gėrybes globalizacijos amžiuje, ypač platesniame nacionalinio saugumo ir kritinės infrastruktūros bei piliečių apsaugos kontekste, pažymėjo, kad būtina identifikuoti, kokią reikšmę saugumo sistemų atsparumas turi bendrame nacionalinio atsparumo ir nacionalinio saugumo kontekstuose. Nors ir pakankamai nedaug išplėtotas, politikos moksluose, per tarptautinių santykių ir saugumo studijų prizmę, atsparumas imtas nagrinėti globalaus valdymo, ekonominio liberalizmo, globalizacijos, darbo rinkos ir valstybės tarnybos reformų kontekste. Taip pat suvereniteto, socialinio kapitalo ir gerovės valstybės nykimo ekonominės liberalizacijos, globalizmo akivaizdoje. Taip pat buvo tyrėjų, nagrinėjančių atsparumą iš NATO vaidmens post-šaltojo karo eros perspektyvoje (Bourbeau, 2013). Be to – atsparumo idėja su jos šaknimis ekologinėse sistemose puikiai dera prie naujos socialinės tvarkos filosofijų, kurios pažymi idėjinį poslinkį nuo tokių reiškinių kaip socialinės struktūros, klasės, valstybės bei stabilus identitetas. Šie reiškiniai, pasak Joseph (2013), išmainomi į tikėjimą nenumatytų atvejų valdymu, sudėtingumu (angl. *complexity*) ir neužtikrintumu. Kaip pažymi Joseph (2013) ir Welsh (2014), atsparumo diskursas yra neoliberalias saugos praktikas skatinantis reiškinys, kuris numato atsakomybes už rizikų valdymą ir reakcijos į jas konceptų poslinkį nuo valstybės link visuomenės. Atsparumo diskursas pažymi rizikos visuomenės proveržį įtraukdamas novatoriškumą, adaptaciją, nenuspėjamumą, transformaciją, pažeidžiamumą ir sistemas į valdysenos diskursą, kuris neužtikrintumo ir nenuspėjamumo valdyseną mato kaip skiriamuosius valdysenos bruožus. Šiame nemažų iššūkių ir nežinomybių kupiname kriziniame periode įvairios atsparumo versijos yra matomos kaip potenciali atsvara ir mobilizuojamos pagerinti archetipines valdysenos technologijas: neoliberalizmo, valdymo per atstumą (angl. *government at a distance*), atsakomybės perkėlimo individams (angl. *responsibilisation*) ir subjektyvavimo (angl. *subjectification*) praktikas, kurios natūralizuotame

neužtikrintumo pasaulyje generuoja tinkamai protingus, autonominius ir antrepreneriškus subjektus (Larner, 2011), formuojančius šiais požiūriais pagrįstus valdymo sprendimus. Kai kurie autoriai apibūdina atsparumo teorijas kaip transformuojančias, normatyvias filosofijas apibrėžiančias pokyčius, sąlygojančius aktyvių piliečių bei savisaugių institucijų atsiradimą (Hopkins 2008; Chandler 2012). Taip pat atsparumas matomas kaip dinaminis procesas, padedantis atsispirti į priekį (Welsh, 2014 iš Shaw 2012;) ir transformuotis į naują darnesnę valstybę. Kiti mano, kad atsparumo įgyvendinimas yra ganėtinai probleminis post-politinės ideologijos reiškinys, susijęs su neoliberalios ekonomikos neužtikrintumu (Duffield, 2011), kai atsparus subjektas yra suvokiamas tokiu iki tol, kol jis adaptuojasi, o ne priešinasi (angl. *resist*) neigiamoms sąlygoms (Reid, 2012). Apžvelgus atsparumo vaidmenį valdymo domene, kyla klausimas, kaip galėtų būti matuojamas atsparumas valdymo sistemų domene įvairiais lygmenimis. Šį klausimą kėlė ir Dahlman (2011), kuri remdamasi neprognozuojamais sistemų griūties pavyzdžiais Egipte, Tunise ar Sovietų Sąjungoje kėlė klausimą, ar gali nacijos, kaip sistemos, atsparumas būti išmatuotas ir, kaip jis galėtų būti stebimas, kokiu būdu galima būtų identifikuoti esminius sisteminius kintamuosius bei gauti ankstyvus įspėjimo signalus apie atsparumo lygio sumažėjimą. Siekiant atsakyti į šiuos klausimus, būtina suvokti kurioje plotmėje yra atsparumo komponentai ir kaip jie gali būti įgaunami ir prarandami. Daliniai matavimai, tokie kaip individualių, nepriklausomų indikatorių nustatymas, nėra tinkamos priemonės – būtina nustatyti įtraukias, integruotas priemones. Iš esmės, atsparumo matavimą komplikuoja tai, kad atsparumas apima vertes, kurios skirtingai suvokiamos skirtingose visuomenėse ar jų grupėse.

1.5.5. Atsparumas kaip kibernetinio saugumo valdymo forma: kibernetinis atsparumas

Kaip pastebi Bryant (2015), organizacijos ir sistemos, nepaisant dedamų didžiulių pastangų jas apsaugoti, ir toliau atakuojamos, todėl vis stiprėja suvokimas, kad ypač sudėtinga, o gal praktiškai neįmanoma, realizuoti konceptą, kai organizacijos apsauga matoma kaip ištisinis visiškai patikimas keliais lygmenimis organizuotas ir nepažeidžiamas perimetras, vien dėl to, kad kiekvienas šio perimetro sluoksnis gali turėti trūkumų arba būti apeitas ryžtingai nusiteikusių įsilaužėlių, o išpuolio rengėjai būti pačios organizacijos viduje. Nagrinėdami kibernetinį atsparumą iš metrikų perspektyvos, Richard ir kt. (2012) pastebėjo, kad nėra tinkamo atsparumo apibrėžimo – tai trukdo išmatuoti faktinį sistemos atsparumą, o egzistuojančios metrikos yra gan kontekstualios ir nepraktiškos. Kaip pažymi Pasaulio ekonomikos forumas (PEF, 2016), kibernetinis atsparumas tampa vis svarbesnis didžiulį susijungimo (angl. *connectivity*) laipsnį turinčiame pasaulyje. Kibernetinis atsparumas apima veiklos praktikas, galimybes absorbuoti atakas, gebėjimus nuo jų atsistatyti ir per kuo trumpesnį laikotarpį atkurti veiklos operacijas. Pagal PEF, tai platesnis požiūris nei kibernetinė sauga, o atsižvelgiant į visą kompleksiškumą – nėra vien IT departamentų rūpestis. Bjorck ir kt. (2015), nagrinėdami kibernetinį atsparumą iš organizacinės perspektyvos, apibrėžė šį reiškinį kaip „gebėjimą nenutrūkstamai teikti numatytus rezultatus, nepriklausomai nuo nepalankių kibernetinių įvykių“. Pagal autorius gebėjimas suvokiamas keliais lygmenimis, kuriuose egzistuoja unikalūs iššūkiai, metodai ir taikytini kontrolės

mechanizmai. Gebėjimas šiame kontekste suvokiamas kaip reiškinys, veikiantis skirtinguose lygmenyse, kai siekiant užtikrinti kibernetinio atsparumo priemonių veiksmingumą ir efektyvumą, kibernetinis atsparumas įgyvendinamas holistiškai, paraleliai skirtinguose lygmenyse. Nenutrūkstamas numatytų rezultatų teikimas turėtų veikti ne tuomet, kai žlunga įprastiniai teikimo mechanizmai. Nenutrūkstamumo aspektas aktualus ir nuolatos keičiant teikimo mechanizmus taip, kad jie gebėtų atsakyti į egzistuojančių rizikų keliamus iššūkius. Tikėtinas rezultatas reiškia, kad analizės vienetas (konkreti sistema) yra pajėgus įgyvendinti elektroninių paslaugų teikimą. Nepalankūs kibernetiniai įvykiai pagal savo kilmę gali būti sąlygoti nenugalimų jėgų (žemės drebėjimai, potvyniai, gaisrai) ar žmogaus veiksmų (kompiuteriniai įsilaužimai, duomenų ištrynimai), arba šių veiksnių derinio. Pagal autorius, į šią kategoriją patenka esminėms informacinių sistemų saugos dimensijoms IT sistemų prieinamumui, vientisumui ar konfidencialumui neigiamą įtaką darantys veiksmai. Iš esmės, kibernetinio atsparumo kontekste šie įvykiai traktuojami kaip normalių operacijų dalis (Bjorck ir kt. 2015).

2012 m. kibernetinio atsparumo svarba akcentuota Pasaulio ekonomikos forumo Davose metu, kai formaliai kibernetinis atsparumas tapo ne tik atskirų individų, verslo ar socialinių grupių susidomėjimo objektu, bet buvo konceptualiai pakylėtas į globalios problematikos nagrinėjimo lygmenį, įtraukiant jį į daugelio šalių kibernetinio saugumo praktikų, politikos ir verslo lyderių darbotvarkes. Nepaisant to, kaip akademinių tyrimų subjektas, jis dar yra pradinėje vystymosi stadijoje – tą rodo labai mažas publikacijų skaičius (Bjorck ir kt. 2015). Pats apibrėžimas yra pakankamai miglotas, o ryškesnį mokslinį progresą ar jo įvertinimą apsunkina metrikų nebuvimas (Ford ir kt., 2012) – o tai, klasikiniais vadybos terminais vertinant, neišmatuojamą reiškinį daro nevaldomu. Akcentuodami kibernetinio atsparumo išmatavimo ir, apskritai, šio reiškinio metrikų suformavimo svarbą, Ford ir kt. (2012) pažymėjo, kad atsparumą sudėtinga apibrėžti, nes terminas apima specifines sistemas, užduotis, rezultatus bei kitas sąlygas, kurios kinta kiekvieno scenarijaus atveju ir užkerta kelią suformuoti universalias matavimo priemones, taikytinas įvairiose sistemose bei įvairiose situacijose. Carnegie Mellon universiteto Programinės įrangos inžinerijos instituto pateikiamame atsparumo valdymo modelyje operacijų atsparumas apibrėžiamas kaip organizacijos gebėjimas adaptuotis prie rizikų, kurios veikia jos esminius operacijų gebėjimus (Allen ir kt., 2011). Pagal modelio autorius, operacijų rizikų valdymas yra paremtas ir įgalintas saugumo, veiklos tęstinumo ir kai kuriais IT operacijų disciplinų aspektais. Atsižvelgiant į tai, kad procesas gali būti apibrėžtas, iškomunikuotas ir kontroliuojamas, jo rezultatai pamatuoti, o visi įmanomi trūkumai identifikuoti. Allen ir kt. (2011) modelyje atsparumo valdymo principus plėtoja per procesinę prizmę, bandydami paaiškinti atsparumo praktikas iš bendros organizacijų procesų perspektyvos. Operacijų atsparumas sąlygoja paslaugos bei su ja susijusių vertybių, apimančių žmogiškuosius išteklius, informacinius resursus, programinę ir aparatinę įrangą, sistemas, gebėjimą įgyvendinti veiklos misiją. Vertinant operacijų perspektyvoje, atsparia paslauga laikytina tuomet, kai ji gali įgyvendinti savo misiją sutrikdymo ar patiriamo stresinio poveikio metu ir gali sugrįžti į įprastinę būseną tuomet, kai sutrikdymas pašalinamas. Priešingai, paslauga laikytina neatsparia, jei ji negali grįžti į normalią būseną po sutrikdymo, nors ir laikinai gali atsilaikyti nepalankiomis sąlygomis. Sistemose, teikiančiose kritines paslaugas, atsparumas matomas kaip keturių esminių gebėjimų visuma:

- planavimas (pasirengimas);
- absorbavimas;
- atsistatymas;
- adaptacija prie žinomų ir nežinomų grėsmių (Hollnagel ir kt. 2011; Linkov ir kt., 2013).

Kalbant apie atsparumą, nemažai sąmyšio kyla iš bandymo prilyginti tvirtumą ir atsparumą, kurie yra susijusios, tačiau skirtingos sistemos savybės. Tvirtumas apibrėžia laipsnį, iki kurio sistema gali atlaikyti netikėto išorinio ar vidinio įvykio arba pokyčio poveikį be sistemos našumo sumažėjimo (Linkov ir kt., 2013). Kita vertus, atsparumas yra sistemos gebėjimas atsistatyti ar regeneruoti jos našumą po netikėto įvykio sistemai sukelto našumo sutrikdymo. Dėl šios priežasties Linkov ir kt. (2013) siūlo vartoti labiau apibendrintus atsparumo konceptus, kurie galėtų būti integruojami su rizikų valdymo požiūriais. Bjorck ir kt. (2015) identifikavo fundamentinius kibernetinio atsparumo komponentus ir išnagrinėjo juos kibernetinio saugumo perspektyvoje, išskirdami penkias esmines kibernetinio atsparumo kategorijas. Vienas svarbesnių aspektų, išskirtas autorių – bendrinio kibernetinio atsparumo apibrėžimo nebuvimas. Autoriai išskyrė šešis skirtingus kibernetinio atsparumo lygmenis. Inžinerijos literatūroje atsparumui įvertinti taikomi metodai dažnai sutelkiami ties vienarūšiais elementais, tokiais kaip tinklo komunikacijų įranga, tačiau realiame pasaulyje tinklai yra sudaryti iš technologinių, socialinių, ekologinių ir ekonominių komponentų ir aplinkos galių, sudarančių integruotą, tarpusavyje informacija besikeičiančią visumą (Linkov ir kt., 2013), todėl atsparumas, būdamas visos šios sistemos savybe, turėtų būti atitinkamai vertinamas ir pozicionuojamas (Linkov ir kt., 2013). Taip Linkov ir kt. (2013) skiria kelių domenų atsparumo modelį, kuriame tam tikru būdu turėtų sklisti informacija. Linkov ir kt. (2013) nuomone, atakos metu sistema iš fizinio domeno perduoda informaciją į kognityvinį lygmenį, t.y. sprendimų priėmėjams. Kognityviniame domene esantys sprendimų priėmėjai naudoja iš fizinio domeno gautą informaciją formuoti atitinkamus uždavinius dėl tolimesnių veiksmų. Pagal autorius, tokia tarpdomeninė informacijos sklaida yra atsparaus sistemos funkcionavimo įvairiuose įvykių valdymo etapuose pagrindas (Linkov ir kt., 2013). Jų nuomone, net ir toks geriau išnagrinėtas reiškinys, kaip rizikos matavimas, kibernetinio saugumo srityje yra pakankamai blogai suvokiamas, o kalbėdami apie atsparumo metrikas kibernetinio saugumo srityje, autoriai pažymi, kad jos apskritai yra nepatenkinamo lygio. Dabartinės egzistuojančios kibernetinių rizikų metrikos yra traktuojamos kaip pasigendančios empirinio validumo (Linkov ir kt., 2013), klaidinančios (Jansen 2009; Bartol ir kt. 2009; Linkov ir kt., 2013) ir dažnai priklauso nuo paprastų heuristinių duomenų, tokių kaip pažeidžiamumų taškų įverčio, trūkstamų klaidų ištaisymų (angl. *patch*), atvirų portų ir pan. Kibernetinio atsparumo matavimo instrumentai turi panašių ir net didesnių trūkumų (Linkov ir kt., 2013). Augantis kibernetinių sistemų sudėtingumas reikalauja rizikų ir atsparumo valdymo procesų integracijos. Kibernetinis atsparumas, savo prigimtimi būdamas lanksčiu reiškiniu, galėtų būti kovos su kibernetinėmis grėsmėmis modelio formavimo parindu ir užtikrinti kritinių kibernetinių vertybių ir paslaugų gyvybiškumą (Linkov ir kt., 2013).

2 lentelė. Kibernetinio atsparumo lygmenys

Lygmuo	Apibūdinimas	Pavyzdys
Viršvalstybinis	Konfederacijos	Europos Sąjunga
Nacionalinis	Šalis ar visuomenė	Švedija
Regioninis	Regionas arba miestas	Stokholmas
Organizacinis	Organizacija	Bendrovė, agentūra, taryba
Funkcinis	Veiklos funkcija	Padalinys, procesas, gebėjimas
Techninis	Techninė sistema	IT sistema, tinklas

Šaltinis: *Bjorck ir kt. (2015)*

Bryant (2015) nagrinėdamas kibernetinio atsparumo konceptus, geresniam reiškinio suvokimui siūlo skirti tris sistemines atsparumo dalis:

- lankstumą;
- sumažintą atakos paviršių;
- gebėjimą dinamiškai atsakyti į atakas.

Bandydami sulyginti kibernetinį saugumą ir atsparumą, Bjorck (2015) ir kt. išskyrė aibę aspektų, išryškinančių šių dviejų reiškinių konceptualią takoskyrą. Toliau vertėtų panagrinėti semantinę autorių analizės dedamąją. Būtina pabrėžti, kad tyrėjai kalba apie dvi pasirinkto objekto sistemines savybes – saugumą ir atsparumą – kibernetinio saugumo kontekste, t.y. nagrinėja jas iš sistemai kylančių kibernetinių grėsmių perspektyvos, t.y., analizuoja konceptualius *kibernetinio saugumo* sisteminio atsparumo bei sisteminio saugumo skirtumus (3 lentelė).

3 lentelė. Kibernetinio saugumo ir atsparumo savybiniai skirtumai

Aspektas	Kibernetinis saugumas	Kibernetinis atsparumas	Komentaras
Tikslas	Apsaugoti IT sistemas, tinklus	Užtikinti veiklos vykdymą	Kibernetinį atsparumą Bjorck pozicionuoja kaip aukštesnio lygmens organizacijos tikslą, kai veiklos vykdymas išorinių ir vidinių suinteresuotų šalių suvokiamas kaip vertės kūrimas, o sistema laikytina atsparia, kai ji gali sukurti vertę net tuomet, jei yra veikiama nepalankių kibernetinių įvykių. Šiuo tikslu, ji naudoja alternatyvias priemones. Taigi, kibernetinio atsparumo perspektyvoje, atskaitos tašku laikytini veiklos procesai, o ne IT.
Intencija	Nesužlugdomumas (angl. *fail safe*)	Saugus žlugti (angl. *safe-to-fail*)	Intencija šiame kontekste apima pageidaujamas sistemos savybes, kibernetinio atsparumo atveju tikimasi, kad esant sistemos žlugimui, jis vyks kontroliuojamu būdu, sistema tuo metu adaptuosis ir atsistatys.
Požiūris	Saugos įgyvendinimas iš išorės	Saugos įgyvendinimas iš vidaus	Kibernetinio saugumo atveju sistemos saugumas užtikrinamas taikant įvairias saugos priemones, tokias kaip šifravimas, kurios

			natūraliai nėra sistemos sudėtinės dalys. Kibernetinio atsparumo požiūris numato saugumo priemones kaip vidines sistemos dalis: integruotas alternatyvias operacijas, dinaminę priemonių kompoziciją.
Architektūra	Vieno lygmens sauga	Kelių lygmenų sauga	Architektūra apima vidines modulines sistemos struktūras ir jų sąsajas. Taikant atsparumo požiūrį jos turėtų būti organizuojamos taip, kad galima būtų išlaikyti dalinį sistemos žlugimą. Todėl architektūrą vertėtų organizuoti keliais apsaugos lygmenimis, o ne vientisu barjeru. Nors tradiciniuose kibernetiniuose sprendimuose taip pat dažnai taikytinas daugiasluoksnės apsaugos konceptas, atsparumo atveju – kiekvienas šių sluoksnių turi būti organizuojamas užtikrinant kuo efektyvesnį jo atsistatymą.
Apimtis	Atomistinis, apimantis vieną organizaciją	Holistiškas, organizacijų tinklas	Atsparumu paremtas požiūris negali iš saugumo perspektyvos vertinti tik vienos konkrečios organizacijos. Būtina įvertinti ne tik viename tinkle sąveikaujančias organizacijas, bet ir tiekėjus. Atsparumu pagrįstas požiūris įvertina ne tik iš kitų tinkle esančių organizacijų potencialiai kylančias grėsmes, bet ir įvertina šių organizacijų stiprybes, kad jas išnaudotų.

Šaltinis: *Bjorck ir kt. (2015)*

Apibendrinant vertėtų išskirti Ford ir kt. (2012) idėjas, kurie pastebėjo, kad sudėtingos kompiuterijos sistemos išgyveno filosofinį jų kūrimo poslinkį nuo principinio orientuoto į tvirtumą link lankstaus ir adaptyvaus dizaino. Tokios sistemos yra pajėgios išgyventi, atsakyti ir atsistatyti nuo išorinių atakų ir vidinių nesėkmių. Toks paradigmos poslinkis link atsilaikymo per dizainą filosofijos yra neišvengiamas, vis labiau ryškėjant proaktyvios gynybos mechanizmų trūkumams. Visuotinai yra pripažįstama, kad sistemų atakavimas yra neišvengiamas ir labai dažnai sėkmingas, todėl jos turi būti formuojamos taip, kad atlaikytų šias atakas bei atsistatytų nuo jų griaunančio efekto bei išlaikytų reikiamus prieinamumo ir funkcionalumo parametrus.

2. KIBERNETINIO SAUGUMO VALDYMO TAIKANT ATSPARUMO POŽIŪRIUS KONCEPTUALAUS MODELIO FORMAVIMAS, TYRIMO METODIKA

2.1. Prielaidos kibernetinio atsparumo modelio formavimui ir struktūrinimui

Pradiniai kibernetinio atsparumo modeliai suformuoti remiantis sintezuojant organizacinio, sistemų ir kibernetinio atsparumo literatūroje išskiriamas atsparumo formavimo idėjas, analizuojant atsparumą formuojančias ir apibrėžiančias savybes, jam užtikrinti būtinas sąlygas. Išsamus kiekvienos modelio komponento sudedamųjų dalių sąrašas pateikiamas lentelėse. Formuojant modelį taikytos struktūrinio funkcionalizmo filosofinės prielaidos, pagal kurias visuomenė – tarpusavyje priklausomų elementų visuma, esanti ekvilibriume arba balanso būsenoje. Laikui bėgant, visuomenė evoliucionavo iš pirmapradės į sudėtingą sistemą, sudarytą iš aukštą specializacijos lygį turinčių elementų. Visuomenės dalys tenkina skirtingas visuomenės funkcijas ir jos poreikius, o bendras vertybių ar vertybių sistemų konsensusas išlaiko visuomenės elementus kartu (Neuman, 2007). Kalbant apie egzistuojančius būdus, naudojamus įvertinti kibernetinio atsparumo sisteminę būklę, pastebėtina, kad gana plačiai paplitęs atsparumo įvertinimo būdas – atsparumo metrikų taikymas. Kaip pažymi Linkov ir kt. (2013), siūlydami atsparumo matavimui taikyti atsparumo matus – egzistuoja pakankamai ryškus skirtumas tarp atsparumo metrikų ir atsparumo matų: atsparumo matai yra kokybinės ar kiekybinės priemonės, skirtos nustatyti specifinės sistemos ar sisteminio komponento atsparumo atributus, savo ruožtu, metrika yra priemonė, skirta palyginti vienos ar daugiau sistemų bei sisteminių, taip pat ir sisteminių komponentų, kokybinius parametrus taikant tam tikrą matą (Albert, Hayes, 2002). Kalbant apie metrikų taikymą, būtina atsižvelgti į tam tikrus specifinius jų aspektus. Kaip rekomenduoja JAV Gynybos departamento Gynybos taryba (2013), atsparumo matavimo metrikos turėtų būti:

- pakankamai plačios ir tinkamos naudoti aibėje skirtingų sistemų;
- preciziškos tiek, kad išmatuotų specifinius sistemų procesus ir komponentus.

Reikėtų pažymėti, kad šie principai taikytini ir formuojant atsparumo matavimo sistemas. Dauguma metrikų, pavyzdžiui Allen ir Curtis (2011) suformuotas CERT Atsparumo valdymo modelis, kuris, anot pačių autorių, yra gan palankiai vertinamas atsparumo mokslinės bendruomenės, ko gero, nėra pats tinkamiausias įrankis tirti atsparumą kontekste, kuriame nėra pakankamai gerai išplėtotas ir reglamentuotas paties reiškinio terminas bei nėra bendro suvokimo, kaip jis turėtų būti matuojamas. Allen ir Curtis (2011) naudojamas CERT modelis, kaip operacijų atsparumo vertinimo ir lygiatyros priemonė iš esmės numato jau suformuotus, pakankamai konkrečius atsparumo elementus, kurie integruoti į įvairius organizacijos valdymo lygmenis ir skirtingas jos operacijų dimensijas. Kadangi šio disertacinio tyrimo atveju tokios sistemos nėra, pasirinkta kokybinio matavimo strategija. Kalbant apie empirinius pagrindus modeliui suformuoti, pažymėtina, kad jie išskirti sintezuojant įvairių atsparumo krypčių atstovų įžvalgas ir bandant koncentruotis ties organizaciniais ir vadybiniais atsparumo aspektais bei į minėtus domenus iš įvairių sričių

perkeliant mobiliuosius atsparumo konstruktus. Organizaciniai atsparumo aspektai įtraukiami iš Gibson ir Tarrant (2010), kurie skiria aibę esminių atsparumo bruožų, nulėmusių konkrečią tyrimo plėtotę:

- atsparumas yra rezultatas, o ne tam tikra sistema jį pasiekti, nors tam tikra nenumatytų atvejų valdymo sistema gali padėti pasiekti atsparumą;
- atsparumas nėra statiškas, bet dinamiškas reiškinys, nuolatos kintantis laike;
- atsparumas nėra vienalytis reiškinys; jis kyla iš daugelio faktorių sąveikos, į kuriuos investuojant tinkamus resursus, organizacijos atsparumo branda kinta nuo reaktyvios būsenos iki proaktyvavus pasirengimo;
- atsparumas yra multidimensinis reiškinys, todėl nėra vieno modelio, kuris galėtų jį paaiškinti;
- atsparumas turi aibę būsenų, kurias skalėje būtų galima atvaizduoti nuo mažiausio atsparumo, kai yra didelis pažeidžiamumas, iki didelio atsparumo laipsnio.

Bishop ir kt. (2011) kritiniu atsparios organizacinės sistemos elementu laiko gebėjimą atsistatyti autonomiškai, t.y. be trečiosios šalies įsikišimo, o tik savo pastangomis. Šios idėjos sąlygoja būtinybę kiekvienai organizacijai identifikuoti šiuos autonominius elementus ir įtvirtinti juos kaip pagrindą, kuriuo remiantis būtų formuojama organizacijos atsparumo sistema. Plėtojant šiuos teiginius atsparumo kritiko Joseph (2013) atsparumo idėjomis, prie atsparumo elementų priskirtini ir gebėjimai atsilaikyti prieš išorines jėgas, šokus ir sutrikdymus, taip pat gebėjimas greitai sugrįžti į savo įprastinę veikimo būseną. Identifikuoti visus šiuos elementus yra kritiškai svarbus uždavinys formuojant atsparumo modelius. Kalbant apie atsparumo sąsajas su organizacijos valdymo ir veiklos organizavimo elementais, būtina suvokti, kaip atsparumas pozicionuojamas organizacijos bendrame bei jos saugumo valdymo praktikų kontekste. Ieškodami minėtų organizacinės sistemos elementų sąsajų, šioje srityje nemažą indelį įnešė Gibson ir Tarran (2010), Aleksic ir kt. (2013). Būtent šiais autoriais remiantis formuojama tyrimo plėtotė bandant išskirti organizacinius atsparumo komponentus. Nagrinėdami organizacinį atsparumą Aleksic ir kt. (2013) identifikavo aibę vidinių ir išorinių organizacijos atsparumo faktorių bei kelis atsparumą įgalinančius faktorius, kurie integruojami su kitų autorių suformuotais atsparumo elementais ir įtraukiami į bendrą atsparumo elementų sąrašą. White (2009) ir Dahlman (2011) pažymi informacijos sklaidos ir informuotumo vaidmenį gerinant organizacinį atsparumą. Star, Newfrock ir Delurey (2003) išskyrė aštuonis fundamentinius klausimus, į kuriuos reikėtų atsakyti norint nustatyti atsparumo būklę organizacijoje. Dalis jų apima atsparumo integraciją į organizacijoje vykdomas programas, dėl to nėra aktualūs konkrečiame tyrimo kontekste, tačiau kita dalimi papildomos tyrimo klausimams plėtoti keliamos tezės. Į modelio struktūros pagrindą įeina McManus (2008) *santykinis bendrojo atsparumo modelis*, kuriuo McManus bandė aprėpti visus įmanomus organizacinio atsparumo indikatorius. McManus (2008) išskyrė tris organizacinio atsparumo faktorius: situacijos žinomumą, esminių pažeidžiamumų valdymą, adaptyvius gebėjimus. Siekiant nustatyti modelio taikymo aplinką, pasinaudota Lee, Vargo ir Seville (2013) idėjomis, kurie atlikę McManus (2008) modelio validaciją, apėmusią teorinį ir ekspertinį vertinimus, išplėtojo faktorius iki keturių, prie jau esamų pridedami ir atsparumo organizacinį etosą.

Kibernetinio atsparumo kultūros formavimas organizacijoje. Adaptuojant McManus (2008) ir Lee, Vargo ir Seville (2013 m,) faktorius pagal tyrimo kontekstą, t.y. pagal kibernetines grėsmes, galima būtų išskirti esmines faktorių plėtotes: atsparumo etosas, organizacinė saugumo ir atsparumo kultūra – šia dalimi siekiama atsakyti į klausimą, kurie bendrieji organizaciniai atributai yra svarbiausi siekiant maksimalaus atsparumo lygio. Atsakymas į šį klausimą padėtų suformuoti geresnį atsparumo pozicionavimo bei atsparios kultūros organizacijoje įžvalgas. Klausimai, į kuriuos būtina atsakyti, siekiant validuoti atsparumo modelį pateikiami 4 lentelėje.

4 lentelė. Atsparumo etoso komponentinės dalies validavimo klausimai

Atsparumo etosas
Kaip galima būtų apibrėžti kibernetinį atsparumą ir kibernetinėms grėsmėms atsparią organizaciją, kokie atributai geriausiai atskleidžia atsparios organizacijos bruožus? Kokie elementai padėtų organizacijai atsilaikyti prieš išorines jėgas, šokus ir sutrikdymus bei pagerintų gebėjimą greitai sugrįžti į savo įprastinę veikimo būseną? Kaip atsparumas turėtų būti integruojamas į egzistuojančius organizacijos saugumo pvz., rizikų valdymo modelius? Ar turi būti vertinamas ir formuojamas atskirai? O gal atsparumas **pats** gali būti integruojantis faktorius veiklos tęstinumui, rizikų ir kibernetinio saugumo valdymui? Kaip atsparumo kultūros formavimą organizacijose galėtų pagerinti: • intitucinės sąrangos pokyčiai; • paskirta už atsparumo gerinimą atsakinga organizacija, departamentas; • bendradarbiavimas su kitomis organizacijomis, sektoriais, piliečiais; • saugumo kompetencijos lygio kėlimas mokymais, kibernetinių atakų imitavimas (angl. *wargaming*), geroji praktika; • kitos veiklos. Ar atsparumo formavimo veiklos galėtų būti išnaudojamos kaip viešojo sektoriaus organizacijų sistemų evoliucionavimą skatinantis reiškinys?

Šaltinis: *sudaryta autoriaus*

Kibernetinio saugumo situacijos žinojimo gerinimas, siekiant padidinti kibernetinį atsparumą. Šia dalimi siekiama atsakyti į klausimą, kurie aspektai yra svarbiausi organizuojant saugumo informacijos sklaidą organizacijoje. Nepaisant pastaruoju metu pakankamai išplėtotų ryšio ir bendradarbiavimo technologijų, informaciniai silosai, kuriuose izoliuojama ne tik bendrinė organizacijos informacija, bet ir su saugumu susiję komunikacijos srautai. Kaip pažymi Lee, Vargo ir Seville (2013), organizacijos gebėjimas komunikuoti tarp organizacinių, socialinių ir kultūrinių ribų indikuoja jų atsparumo būklę. Endsley ir kt. (2003) situacijos žinojimą apibrėžia kaip žinojimą, kas vyksta aplink ir suvokimą, ką tai reiškia dabar ir ateityje. Remiantis šiomis įžvalgomis suformuotas modelio komponentas.

5 lentelė. Situacijos žinojimo komponentinės dalies validavimo klausimai

Kibernetinio saugumo situacijos žinojimas
Kaip turėtų būti organizuojamas kibernetinio saugumo situacijos žinojimas, siekiant padidinti viešojo sektoriaus organizacijų kibernetinį atsparumą?

Kaip geriausiai būtų organizuoti išvardintas veiklas, siekiant padidinti kibernetinį atsparumą:
- darbuotojų kibernetinių incidentų metu vykdomų funkcijų žinojimo gerinimas;
- bendras kibernetinio atsparumo problemų suvokimo gerinimas;
- išorinių ir vidinių procesų, sektoriaus stebėsena ir jos rezultatų sklaida suinteresuotoms šalims;
- darbuotojų tarpusavio interakcijų saugumo klausimais dažnumo didinimas;
- kibernetinių rizikų pasekmių ir poveikio suinteresuotoms šalims (paslaugų gavėjai, kitos organizacijos) žinojimo gerinimas;
- ekspertinės pagalbos saugumo klausimais teikimas vienos organizacijos kitai gerinimas;
- gerųjų atsparumo praktikų sklaida;
- ankstyvojo krizių perspėjimo mechanizmų formavimas;
- kitos veiklos.

Šaltinis: *sudaryta autoriaus*

Esminių (angl. *keystone*) kibernetinių pažeidžiamumų valdymas, siekiant padidinti kibernetinį atsparumą. Šios srities identifikavimas ir sąsajos didžiąja dalimi sietinos su McManus, Seville, Vargo bei Stephenson (2008, 2009, 2010) atsparumo studijomis Naujosios Zelandijos organizaciniame domene. Ši sritis apima pažeidžiamumų, keliančių grėsmę organizacijos išgyvenimui identifikavimą, proaktyvų jų valdymą ir su jais susijusį reagavimą. Į šią sritį įeina krizių ir katastrofų valdymas bei planavimas, veiklos tęstinumas.

6 lentelė. Esminių kibernetinio saugumo pažeidžiamumų valdymo komponentinės dalies validavimo klausimai

Esminių pažeidžiamumų valdymas
Kaip turėtų būti organizuojamas esminių pažeidžiamumų valdymas, siekiant padidinti viešojo sektoriaus organizacijų kibernetinį atsparumą? Kaip geriausiai būtų organizuoti išvardintas veiklas, siekiant padidinti kibernetinį atsparumą: • su esminiais pažeidžiamumais susijusių nenumatytų atvejų ir kibernetinių incidentų veiklų pozicionavimas aukščiausiame organizacijos valdymo lygmenyje; • kibernetinių pažeidžiamumų aptikimo potencialo didinimas; • vertybių (angl. *assets*) ir paslaugų kategorizavimas pagal jų svarbą, išskiriant kritines paslaugas ir vertybes. • kitos veiklos.

Šaltinis: *sudaryta autoriaus*

Adaptyvumo gerinimas siekiant padidinti kibernetinį atsparumą. Šia komponentine dalimi siekiama atsakyti į klausimą, kokie veiksniai yra svarbiausi formuojant adaptyvias organizacines struktūras. Dažnai literatūroje adaptyvumas pripažįstamas vienu iš kertinių atsparumo elementų, tačiau, kaip rodo praktinės situacijos analizė, organizacijos nepasimoko iš saugumo klaidų, sistemos po tam tikrų saugumo incidentų ir toliau apsaugomos nepakankamai, nevykdoma sisteminė jų rekonfigūracija, procesiniai pakeitimai, galintys padėti išvengti pasikartojančių saugumo incidentų ateityje. Pagal Lee, Vargo ir Seville (2013), organizacijos gebėjimas adaptuotis konceptualiai yra visų jos atsparumo gebėjimų visumos centre. Kitaip kalbant, adaptyvumas yra organizacinio atsparumo pamatas.

7 lentelė. Organizacinės sistemos adaptyvumo gerinimo komponentinės dalies validavimo klausimai

Organizacinės sistemos adaptyvumas
Kaip turėtų būti didinami adaptyvūs institucijų gebėjimai, siekiant padidinti viešojo sektoriaus organizacijų kibernetinį atsparumą? Kaip geriausiai būtų organizuoti išvardintas veiklas, siekiant padidinti kibernetinį atsparumą: • judėjimo nuo reaktyvaus modelio link proaktyvaus pasirengimo ir galiausiai link didelio nežinomumo lygio adaptavimosi gerinimas; • institucijų gebėjimų veikti krizinėmis sąlygomis (sprendimų priėmimas ir pan.) gerinimas; • krizinių situacijų peržiūra po kibernetinio incidento siekiant pasirengti panašaus pobūdžio įvykiams ateityje; • kitos veiklos.

Šaltinis: *sudaryta autoriaus*

Sistemos lankstumo gerinimas, siekiant padidinti kibernetinį atsparumą. Lankstumas yra pakankamai senai naudojamas sistemų atributas ir taikomas visų rūšių sistemose, pradedant gamybinėmis, baigiant socio-kibernetinėmis. Tai platus tyrimo laukas, apibūdinantis sistemos gebėjimą adaptuotis išoriniams pokyčiams. Kalbėdami apie kibernetines sistemas, Gebauer ir Schober (2006) pažymi, kad norėdama būti efektyvia, sistema privalo būti lanksti, tačiau per didelis lankstumas, autorių nuomone, gali neigiamai atsiliepti sistemos vartotojų patirčiai. Kalbant apie lankstumo pradą kibernetinės erdvės, kaip sociotechninės sistemos kontekste, pažymėtina, kad, be jokios abejonės, jis kyla iš žmogiškojo kibernetinės sistemos elemento, kuris nulemia kaip turėtų būti organizuojamos kompiuterijos sistemos, kokius uždavinius jos turi atlikti. Žmonės taip pat gali nustatyti technologijomis užtikrinamo lankstumo laipsnį. Lankstumas saugos kontekste yra visiškai priešinga sąvoka efektyvumui. Pavyzdžiui, iš efektyvumo perspektyvos yra žymiai geriau naudoti vienodą, kompiuterijos įrangą, nes taip pasiekiama standartizacija, kuri, modernių technologijų kompleksiškumo kontekste, matoma kaip turinti didžiulę įtaką inovacijoms, produktyvumui bei rinkos struktūroms (Tassey, 1999). Tačiau, diskutuojant apie sistemos lankstumą ir bendrąjį atsparumą, verta pastebėti, kad kuo sistemos techniniai komponentai labiau standartizuoti, suvienodinti, tuo labiau vieno iš šių komponentų saugos spragos įtakoja kitus sistemoje esančius elementus. Savaime suprantama, kad sistema negali būti visiškai heterogeniška, nes, priešingu atveju, iškylą grėsmė jos skirtingų komponentų integracijai, kas sąlygoja darnios jos veiklos sutrikdymus, todėl kritiškai svarbu išlaikyti šių dviejų konceptų pusiausvyrą (Bryant, 2015).

8 lentelė. Organizacinės sistemos lankstumo didinimo komponentinės dalies validavimo klausimai

Sistemos lankstumo didinimas
Kaip turėtų būti didinamas sistemų lankstumas, siekiant padidinti viešojo sektoriaus organizacijų kibernetinį atsparumą? Kaip geriausiai būtų organizuoti šias veiklas, siekiant padidinti kibernetinį atsparumą: • procesų projektavimas taip, kad esant krizinei situacijai juos galima būtų pertvarkyti; • sistemos formavimas laikantis modulinio principo;

- sistemos komponentų įvairovės didinimas;
- sistemos pertvarkymas atsižvelgiant į aplinkos sąlygas;
- kitos veiklos.

Šaltinis: *sudaryta autoriaus*

Organizacinės sistemos atakos paviršiaus mažinimas. Kibernetinės sistemos atakos paviršiaus mažinimas yra ypač aktualus įvairiais aspektais: tiek siekiant plėtoti įvairias kibernetinių sistemų formas, pradedant debesų kompiuterija (Szefer ir kt., 2011), baigiant mobiliomis platformomias (Bartel ir kt., 2013), tiek didėjant socialinės inžinerijos atakoms, atsižvelgiant į žmogiškąjį faktorių bei žmogiškąjį atakos paviršių. Kalbėdami apie sistemos atakos paviršių, Manadhata ir Wing (2005, 2011) pažymi, kad sistemos atakos paviršiaus puolamumas gali būti išreiškiamas trimis dimensijomis: metodu, duomenimis ir kanalu, ir apskritai– kuo didesnis sistemos atakos paviršius, tuo didesnė tikimybė, kad ji bus atakuota, vadinasi – nesaugesnė. Atakos paviršius apima visus potencialius sistemos prieigos taškus, kuriuos gali išnaudoti išpuolį rengiantys subjektai, todėl kibernetinės saugos operatoriams būtina jį kiek įmanoma sumažinti, taip jį padarant kiek įmanoma atsparesniu. Atsižvelgiant į tai, kad vis dažniau reikalaujama, jog programinė įranga atliktų kuo daugiau funkcijų, o tai dažnai apima įvairių komunikacijos kanalų išnaudojimą – šios užduoties įgyvendinimas yra pakankamai sudėtingas. Iš programinės įrangos perspektyvos, ji gali būti įgyvendinama mažinant naudojamų programų skaičių organizacijose, nes kiekviena programa sukuria papildomos grėsmės tikimybę. Iš aparatinės įrangos pusės, atakos paviršius gali būti mažinamas atsisakant nereikalingų komunikacijos portų ir kanalų, ribojant bevielio tinklo aprėptį, taip pat informacijos perdavimo portų, tokių kaip USB, naudojimą bei segmentuojant saugos lygius tinkle. Bet kokie apribojimai sukelią trintį tarp vartotojų poreikių ir saugos reikalavimų, tačiau šiame etape taip pat būtina surasti balansą, priklausomai nuo organizacijos reikalavimų saugai (Bryant, 2015). Atakos paviršius apibrėžiamas kaip sistemos atskleistųjų (angl. *exposures*) vietų visuma, galinti būti išnaudota (Hubbard ir Seiersen, 2016) prieš sistemą vykdyti atakas[28]. Kaip pažymi Hubbard ir Seiersen (2016), viena dalis egzistuojančių atakos paviršiaus apibrėžimų apima sisteminius, kita dalis – tinklo infrastruktūros atakos paviršius, tačiau nei vienas jų nėra pakankamai platus konceptualizuoti net konkrečios organizacijos atakos paviršių. Atsižvelgiant į tai, autoriai siūlo išskirti organizacijos (angl. *enterprise*) atakos paviršių, kuris apimtų visus konkrečios bendrovės tinklus, sistemas bei trečiąsias šalis, esančias organizacijos ekosistemoje: organizacijos paslaugų vartotojus, tiekėjus ir pan. Be šio mikro lygmenyje esančio atakos paviršiaus egzistuoja ir kitas makro lygmenyje egzistuojantis globalusis atakos paviršius, sąlygojamas keturių esminių elementų: globalaus interneto ir elektroninių paslaugų naudotojų skaičiaus, šių naudotojų įvairovės, atrastų ir išnaudotų pažeidžiamumų skaičiaus. Globalus atakos paviršius apima visą aibę visose valstybinėse, privačiose ir piliečių naudojamose sistemose esančių atskleistųjų vietų (angl. *exposures*) ir su kiekvienu nauju interneto vartotoju, nauja internetine svetaine ar nauju įrenginiu, prisijungtu į globalų tinklą atakos paviršius vis labiau plečiasi. Aukštas informacinės visuomenės susijungimo

28 https://cve.mitre.org/about/terminology.html

lygis bei didėjanti piliečių, verslo ir valdžios institucijų priklausomybė nuo kibernetinės infrastruktūros sąlygoja naujų, nenumatytų ir nežinomų grėsmių atsiradimą, atveria kelius kibernetinėms atakoms, vidinėms ir išorinėms grėsmėms bei pažeidžiamumams tiekimo grandžių tinkluose (*Department of Defense*, 2011; Linkov ir kt., 2013). Dėl didėjančios prisijungimo technologijų įvairovės daugėja ir būdų juos išnaudoti (angl. *exploit*) bei tą daryti bandančiųjų skaičius, kuris dažnai įgauna organizuoto nusikalstamumo bruožus, inicijuojamus net ir vienos kitai priešiškai nusiteikusių valstybių. Taip artėjama prie globaliojo atakos paviršiaus išsiplėtimo istorinio maksimumo, kai net pačiai organizacijai esant pakankamai saugiai, gali būti pažeistas ir išnaudotas jos tiekėjų saugumo spragos (Hubbard ir Seiersen 2016). Instinktyviai bandydami apsisaugoti nuo išpuolių sistemų valdytojai ir už sistemų saugumą atsakingi ekspertai bando sutvirtinti sistemas, atsisakant nereikalingų elementų, tokių kaip programinė įranga, duomenys, privilegijos ir pažeidžiamumai. Tokie veiksmai, nors ir pastoviai reikalauja vis didesnių resursų, sumažina, tačiau visiškai nepašalina atakos paviršiaus (Hubbard ir Seiersen 2016).

9 lentelė. Organizacinės sistemos atakos paviršiaus mažinimo komponentinės dalies validavimo klausimai

Organizacinės sistemos atakos paviršiaus mažinimas
Kaip turėtų būti įgyvendinamas organizacinės sistemos atakos paviršiaus mažinimas, siekiant padidinti viešojo sektoriaus organizacijų kibernetinį atsparumą? Kaip geriausiai būtų organizuoti šias veiklas, siekiant padidinti kibernetinį atsparumą: • Naudojamos programinės įrangos tvarkos griežtinimas? • Nereikalingų komunikacijos kanalų atsisakymas? • Organizacinės sistemos sudėtingumo lygio mažinimas? • Darbuotojų mokymai apie socialinę inžineriją, saugumą ir pan.? • Prieigos prie sistemų „taškų“ (angl. *entry points*) mažinimas? • Kitos veiklos?

Šaltinis: *sudaryta autoriaus*

Reakcijos į atakas gerinimas. Bendrame kibernetinio saugumo kontekste reakcijos į atakas gerinimas yra pakankamai nemažą teorinę istoriją turintis procesas, kuriuo jau praėjusio šimtmečio pabaigoje Brackney (1998) siūlė praplėsti egzistuojantį JAV Gynybos departamento trijų lygmenų (apginti (angl. *protect*), detektuoti (angl. *detect*), reaguoti (angl. *react*)) gynybinį informacinių operacijų modelį. Jis ypač aktualus vykstant socio-fizinių ir kibernetinių sistemų konvergencijai, kai vis dažniau kalbama, jog reaguojant į kibernetines atakas galimas ir konvencinių karinių priemonių taikymas[29]. Tačiau neplėtojant fizinių-karinių priemonių, kurių pritaikymas būtų pakankamai sudėtingas, vien dėl greito tikslaus užpuoliko nustatymo sudėtingumo bei tikimybės, kad atakos nebūtinai turėtų būti organizuojamos piktavališkai nusiteikusių šalių, o pavienių asmenų, visų pirma, reakcijas į atakas vertėtų nagrinėti iš kibernetinio atsako priemonių perspektyvų. Toks reakcijos į atakas nagrinėjimas vykdomas atsparumo ir sistemos atsistatymo greičio didinimo poreikio kontekste, vertinant atsistatymo dedamąsias, kurios galėtų padėti sistemai kuo greičiau sugrįžti

29 http://www.telegraph.co.uk/news/2017/06/27/cyber-attack-could-lead-military-retaliation-says-fallon/

į jos ankstesnę būseną. Taip, kalbėdamas apie šias priemones, Brackney (1998) kelia aibę klausimų: kiek reikalingas atsako koordinavimas, kiek atsakas gali būti automatizuojamas, kokie analizės ir įspėjimo mechanizmai gali būti taikomi, kokie bendrai yra atsako pasirinkimai. Reakcijos į atakas gerinimo procesai sudaro atsparumo modelių, turinčių absorbavimo fazę, šios fazės esmę. Bryant (2015) siūlo organizacijose užtikrinti atsparumą jas valdant labiau kaip manevruojančias dinamiškas pajėgas nei kaip IT padalinius, kurių dabartiniai komandiniai padaliniai turi pernelyg sudėtingas, vertikalėje ypač ištemptas sprendimų priėmimo struktūras. Egzistuoja būdų kontratakuoti įsilaužėlius, tačiau tai yra neteisėtos ir iš etinės pusės diskutuotinos priemonės, daug mažiau problematiška iš teisinės pusės yra įrengti taip vadinamus „medaus puodus" (angl. *honey pots*) – dirbtinai sukurtas nesaugias sistemines dalis, kurios pritraukia įsilaužėlius, taip gaišinamas jų laikas, jiems pateikiama suklastota ir netiksli informacija. Tokiu būdu, švaistomi išpuolį rengiančio subjekto resursai. Kaip pastebi Bryant (2015), iš esmės didžiausia grąža iš įdirbio formuojant kibernetinės saugos atsparumą gaunama per personalo atsparumo formavimą.

10 lentelė. Reakcijos į atakas gerinimo komponentinės dalies validavimo klausimai

Reakcijos į atakas gerinimas
Kaip turėtų būti gerinami esami reakcijos į atakas mechanizmai, siekiant padidinti viešojo sektoriaus organizacijų kibernetinį atsparumą? Kaip geriausiai būtų organizuoti šias veiklas, siekiant padidinti kibernetinį atsparumą: • Reakcijos į atakas tvarka ir procesai, koordinavimas? • Bendriniai reakcijos į atakas klausimai: • Duomenų pakeitimas atsarginėmis kopijomis? • Kibernetinių incidentų pasekmių šalinimo tvarka? • Pasyvių priemonių kibernetiniams nusikaltėliams privilioti (angl. *honey pots*) formavimas? • Pažeistų sistemos komponentų izoliavimo tvarka? • Kitos veiklos

Šaltinis: *sudaryta autoriaus*

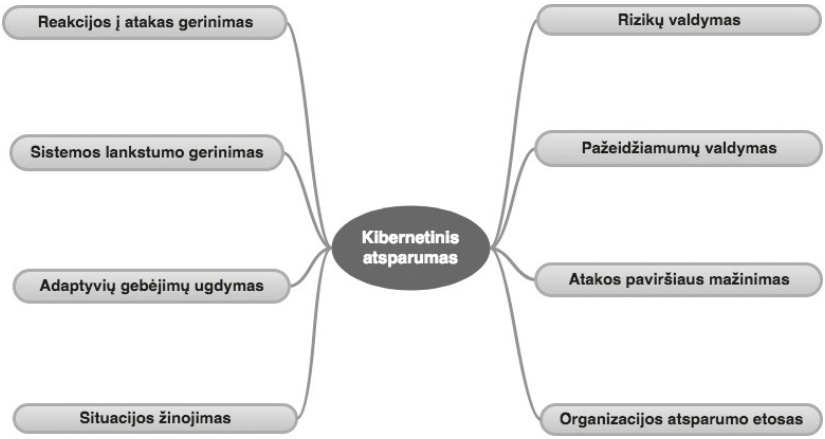
Rizikų valdymas. Šia tyrimo dalimi siekiama atsakyti į klausimą, kurie rizikų valdymo aspektai yra svarbiausi siekiant sukurti atsparią organizaciją. Pagal Gibson ir Tarrant (2010), atsparumas prasideda tinkamu rizikų valdymu, todėl kritiškai svarbu yra kuo giliau suvokti šią sritį. Atsparumo kibernetinėms rizikoms kontekste ypač plačiai nagrinėjami technologiniai rizikų faktoriai, tačiau organizaciniai aspektai nėra taip dažnai sutinkami literatūroje. Sudėtingėjančios kibernetinės sistemos ir kibernetinės grėsmės reikalauja rizikų valdymo ir atsparumo valdymo procesų integracijos (Linkov ir kt., 2013). Kaip nustatė Kraemer, Carayon ir Clem (2008), organizaciniai rizikų faktoriai vaidina reikšmingą vaidmenį kompiuterių ir informacijos saugumo srityje, o pagal prigimtines savybes juos galima suskirstyti į devynias kategorijas: išorinės įtakos, žmogiškosios klaidos, valdymas, organizavimas, našumo ir resursų valdymas, politiniai klausimai, technologijos ir personalo mokymai.

11 lentelė. Rizikų valdymo komponentinės dalies validavimo klausimai

Rizikų valdymas
Kaip turėtų būti įgyvendinamas rizikų valdymas, siekiant padidinti viešojo sektoriaus organizacijų kibernetinį atsparumą? Kaip geriausiai būtų organizuoti šias veiklas, siekiant padidinti kibernetinį atsparumą: • Rizikų valdymo gairių parengimas, palaikymas? • Rizikų vertinimo mechanizmų tobulinimas? • Rizikų aibės formavimas, nuolatinis atnaujinimas pagal egzistuojančias aplinkybes? • Išorinių auditų atlikimas? • Kitos veiklos?

Šaltinis: *sudaryta autoriaus*

Apibendrinta pradinė kibernetinio atsparumo modelio struktūra pateikiama 12 pav.



Šaltinis: *parengta autoriaus*

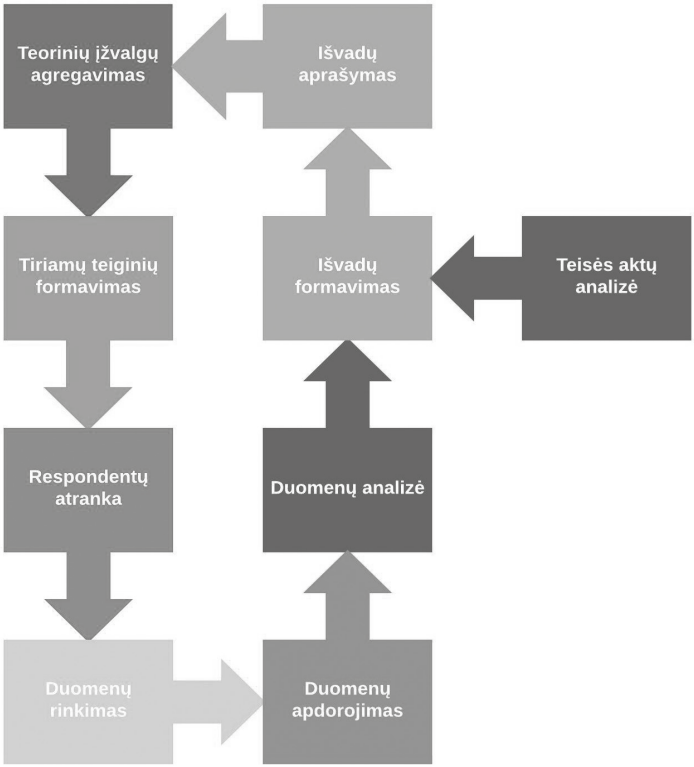
12 pav. *Kibernetinio atsparumo modelio struktūra*

2.1.1. Tyrimo metodika

Literatūroje egzistuoja aibė tyrimo proceso skirstymo į etapus būdų. Adaptuojant Augustinaičio, Rudzkienės, Petrausko su kolegomis (2009) ir Bryman (2012) siūlomus tyrimo etapus, visas procesas skirstytinas į aštuonis pagrindinius etapus:

1. Teorinių įžvalgų formavimas – apima mokslinės problemos formulavimą, tikslų ir uždavinių nustatymą bei apibrėžimą.
2. Tiriamųjų teiginių formavimas – apima metodo parinkimą ir vertinimo kriterijų nustatymą, teiginių formavimą ir grupavimą.
3. Interviu dalyvių atranka – apima ekspertų grupės sudarymą.
4. Duomenų rinkimas – informacijos gavimas.
5. Duomenų apdorojimas – duomenų parengimas analizei.

6. Duomenų analizė – ekspertų interviu metu surinktų duomenų ir teisės aktų analizė.
7. Išvadų formavimas – atliekamas sintezuojant ankstesniuose tyrimo etapuose gautus rezultatus.
8. Išvadų aprašymas – apima gautų rezultatų apibendrinimą išvadų ir siūlymų pateikimą.



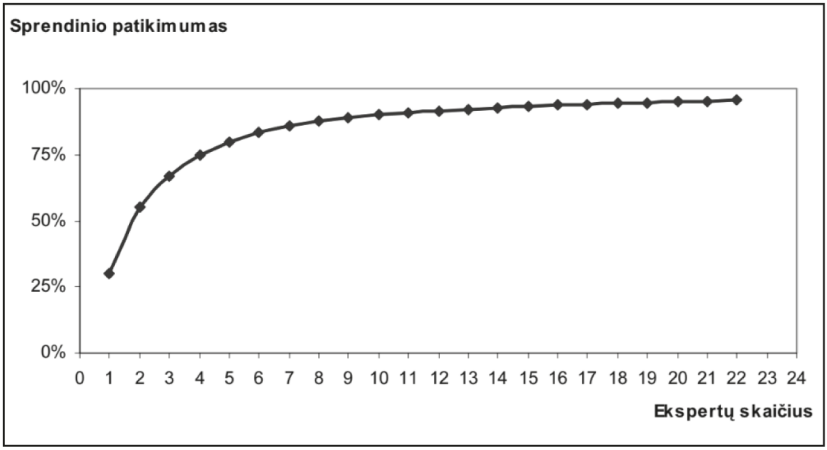
Šaltinis: *parengta autoriaus pagal Augustinaitį, Rudzkienę, Petrauską ir kt. (2009); Bryman (2012)*

13 pav. *Pagrindiniai tyrimo etapai*

2.1.2. Ekspertų interviu

Tyrimo imtis, ekspertų atranka. Tyrimo ekspertų atrankai taikyta tikslinė ekspertų atranka, kuri paprastai naudojama tokiose situacijose, kai atvejai atrenkami turint tam tikrą tikslą. Tokio pobūdžio atranka taikoma žvalgomuosiuose ir lauko tyrimuose. Tikslinė atranka yra tinkama tuomet, kai tyrėjas siekia identifikuoti tam tikrus atvejus bei egzistuojant tikslui gauti ne didesnės populiacijos apibendrintą vaizdą, bet gilesnę tam tikros tipinės

grupės analizę. Ekspertai atrenkami konkrečiu tikslu, kad savo žiniomis prisidėtų prie problemos ar uždavinio sprendimo. Ekspertams keliami reikalavimai siejami su tiriamos srities kompetencija ir patirtimi (Augustinaitis, Rudzkienė, Petrauskas ir kt., 2009). Kalbant apie ekspertų kompetenciją, reikia pažymėti, kad tyrimui atrenkami ekspertai, kurie tik šiuo atveju įtraukiami į problemos sprendimą todėl, kad nėra kitokių informacijos gavimo būdų ir objektyvus matavimas negalimas arba netikslingas. Kalbant apie ekspertų patikimumą, reikėtų pastebėti, kad ekspertizės patikimumas dažniausiai įvertinamas tik remiantis po bandymo gautais rezultatais. Kaip pažymi Augustinaitis, Rudzkienė, Petrauskas ir kt. (2009), daugelio mokslininkų nuomone, optimalus grupės dydis yra nuo 8 iki 10 ekspertų. Nepaisant to, kad šio tyrimo atveju apklaustas mažesnis skaičius (7 ekspertai), gautas pakankamas kiekis duomenų analizei, pasiektas pakankamas teorinio prisisotinimo lygis. Tokio ekspertų skaičiaus patikimumas pagal Augustinaitį, Rudzkienę, Petrauską ir kt. (2009) siekia apie 90%. Ekspertų patikimumo nustatymas pagal jų skaičių pateikiamas 14 paveiksle.



Šaltinis: *Augustinaitis, Rudzkienė, Petrauskas ir kt. (2009)*
14 pav. *Ekspertų skaičiaus įtaka vertinimo patikimumui*

Ekspertų charakteristikos. Tyrime dalyvavę kibernetinio saugumo ekspertai yra valstybiniame sektoriuje dirbantys valstybės tarnautojai, buvę ir šiuo metu esantys statutiniai pareigūnai. Dauguma apklaustų ekspertų yra prisidėję prie kibernetinio saugumo sistemos formavimo nuo pat jos ištakų, dalyvavę ir šiuo metu dalyvaujantys rengiant teisės aktus bei formuojant šios srities politiką Lietuvoje. Kadangi didžioji dalis ekspertų išreiškė norą dalyvauti tyrime anonimiškai, jiems priskirti idendifikavimo kodai, kurie pateikiami 12 lentelėje.

12 lentelė. Ekspertų ir interviu informacija

Eksperto kodas	Interviu data	Interviu trukmė
E1	2017-07-11	120 min
E2	2017-07-14	33 min
E3	2017-07-21	38 min
E4	2017-07-24	46 min
E5	2017-07-24	50 min
E6	2017-07-26	43 min
E7	2017-08-14	40 min

Šaltinis: *sudaryta autoriaus*

2.1.3. Kibernetinio atsparumo principų formalizavimas kibernetinio saugumo teisės aktuose Lietuvoje – tyrimo metodika

Nagrinėjant organizacinio atsparumo literatūrą bei atliekant ekspertinį tyrimą, daroma prielaida, kad nepaisant to, jog kibernetinis atsparumas neįvardinamas tiesiogiai, tačiau įgyvendinant tam tikrus kibernetinio saugumo principus stiprinamas ir kibernetinis atsparumas. Siekiant nustatyti kokiu mastu LR kibernetinį saugumą ir gretutines sritis reglamentuojančiuose teisės aktuose įtvirtinami atsparumo principai, atlikta šių teisės aktų analizė. Analizei atlikti buvo remiamasi PEF, Linkov, NIST kibernetinio atsparumo matrica, literatūros analizės ir ekspertinio interviu metu identifikuotais atsparumo aspektais. PEF, Linkov, NIST atsparumo matricą sudaro keturios dimensijos: fizinė, informacinė, kognityvinė ir socialinė. Kiekviena šių dimensijų turi penkis lygius, kurių kiekvieną sudaro aibė uždavinių. Ši matrica gali būti taikoma tiek vertinti esamam atsparumo lygiui, tiek kaip modelis formuoti atsparumui naujoje kibernetinio saugumo sistemoje. Matricoje sintezuojami JAV Nacionalinės mokslo akademijos (2012) suformuoti atvejų valdymo cikle išskiriami keturi lygmenys, kuriuos sistema turi plėtoti, norėdama išlaikyti atsparumą. Prie kiekvieno valdymo ciklo elemento laužtiniuose skliaustuose pridedamas jo kodas, kuris bus taikomas atliekant gautų rezultatų analizę – grupuojant elementus pagal jų svarbą, t.y. identifikuojant kiekvieno ciklo elementų pasikartojimo dažnį ir taip siekiant nustatyti jų prioritetiškumą. Šie lygiai yra:

- planavimas, pasirengimas (angl. *plan, prepare*) – paslaugų prieinamumo pagrindo formavimas siekiant nenumatytų atvejų metu paslaugas išlaikyti prieinamomis, o vertybes funkcionaliomis;.
- absorbavimas (angl. *absorb*) – pačių kritiškiausių vertybių funkcionavimo ir paslaugų prieinamumo palaikymas, sutrikdymo suvaldymo metu.
- atsistatymas (angl. *recover*) – visų vertybių funkcionavimo ir paslaugų prieinamumo atstatymas į prieš nepageidaujamą įvykį egzistavusią būseną.
- adaptacija (angl. *adapt*) – įvykio žinių naudojimas pakeisti sistemos protokolą, konfigūraciją, personalo apmokymo principus ar kitus sistemos valdymo aspektus siekiant padidinti jos atsparumą.

Šiuos keturis elementus taikę Linkov ir kt. (2013) sintezavo juos su Alberts, Gartska, Stein (2000) ir „Tinklinės karybos doktrinoje“ identifikuotais domenais suformavo kibernetinio atsparumo matricą. Alberts, Gartska, Stein (2000) nustatyti domenai yra šie:

- fizinis – fiziniai resursai ir gebėjimai bei šių resursų kūrimo galimybės;
- informacinis – bendroji ir fizinio domeno informacija;
- kognityvinis – informacinio ir fizinio domeno naudojimas sprendimams priimti;
- socialinis – organizacinė struktūra ir komunikacija, kognityviniams sprendimams priimti.

Vėliau kibernetinio atsparumo matrica, peržiūrėta ir praplėsta PEF, Linkov, NIST ekspertų, įgavo galutinę formą, pavaizduotą lentelėje, pateikiamoje priede Nr. 3. Atliekant tyrimą didžiausias susidomėjimas skiriamas informaciniam, kognityviniam ir socialiniam domenui. Šio domeno elementai konceptualiai apjungiami su McManus (2008) bei Lee, Vargo ir Seville (2013) organizacinio atsparumo modelio elementais. Persidengiantys ar neaktualūs elementai atmetami. Konstrukciškai visi teiginiai suskirstyti laikantis Lee, Vargo ir Seville (2013) keturių organizacinio atsparumo domenų struktūros juos papildant. Siekiant nustatyti kaip LR kibernetinio saugumo teisės aktuose perteikiami atsparumo principai, sudaryta svarbiausių šios srities teisės aktų sąrašas, pateikiamas 13 lentelėje.

13 lentelė. LR Kibernetinį saugumą reglamentuojantys teisės aktai

Teisės akto pavadinimas	Teisės akto priėmimo data, numeris, priėmimo vieta
Lietuvos kibernetinio saugumo įstatymas	2014 m. gruodžio 11 d. Nr. XII-1428 Vilnius
Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas	2011 m. gruodžio 15 d. Nr. XI-1807 Vilnius
Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programa	2011 m. birželio 29 d. Nr. 796 Vilnius
Nacionalinis kibernetinių incidentų valdymo planas	2016 m. sausio 25 d. Nr. 87 Vilnius
Bendrųjų elektroninės informacijos saugos reikalavimų aprašas	2013 m. liepos 24 d. Nr. 716 Vilnius

Šaltinis: *sudaryta autoriaus*

Kiekvienas teisės aktas išnagrinėtas atskirai lyginant jame išdėstytus kibernetinio saugumo principus su įvairių PEF, Linkov, NIST matricos dimensijų ir jų dalių kibernetinio atsparumo uždaviniais.

3. KIBERNETINIO SAUGUMO VALDYMO TAIKANT ATSPARUMO POŽIŪRIUS EMPIRINIO TYRIMO REZULTATAI

3.1. Kibernetinio atsparumo etoso formavimas

Tyrimo metu, atliekant interviu, visų pirma, buvo bandoma nustatyti: kaip Lietuvos kibernetinio saugumo ekspertai suvokia kibernetinį atsparumą; kaip jie apibūdintų kibernetinėms grėsmėms atsparią organizaciją; kaip atsparumas turėtų būti pozicionuojamas kitų kibernetinio saugumo formavimo procesų atžvilgiu. Pažymėtina, kad dėl didelio kibernetinio saugumo tarpdisciplininiškumo masto ir pakankamai turtingos bei neretai painios egzistuojančios kibernetinio saugumo ir gretutinių sričių terminijos, ypač akcentuotinas kibernetinio atsparumo pozicionavimas bendroje kibernetinio saugumo sąvokų ontologijoje. Identifikavus ir apibrėžus tiriamo reiškinio suvokimo ribas, toliau galima kelti klausimus: „Kokiomis priemonėmis jis galėtų būti gerinamas?; Kokie pokyčiai reikalingi, siekiant suformuoti atsparumo požiūriu pagrįstą kibernetinio saugumo kultūrą Lietuvos viešajame sektoriuje?“.

Kibernetinio atsparumo sąvoka, kibernetinėms grėsmėms atspari organizacija. Pažymėtina, kad išnagrinėjus literatūros šaltinius, akivaizdu, kad nėra universalios, visiems kibernetinio saugumo sistemos dalyviams vienodai suprantamos kibernetinio atsparumo sąvokos. Tai matoma ir apibendrinus tyrime atliktų interviu metu ekspertų pateiktus atsakymus. Nustatyta, kad kibernetinis atsparumas gali būti vertinamas iš kelių organizacijoje vykstančių kibernetinio saugumo procesų perspektyvų akcentuojant vienokius ar kitokius sisteminius atsparumo bruožus:

1. Kibernetinio atsparumo suvokimas, taikant požiūrius, apimančius tam tikrą konkrečiai apibrėžtą sociotechninių sistemų komponentą – ryšio tinklus. Tačiau, kalbant apie jo įgyvendinimo mastą, toks suvokimas kibernetinį atsparumą vertina ne tik iš organizacinės, bet iš daug platesnės – nacionalinės perspektyvos. Kibernetinio atsparumo objektui kylančios grėsmės neapsiriboja vien kibernetinėmis, tačiau apima ir papildomus pavojus: elektros tiekimo sutrikdymus, žmogiškas klaidas bei kitus tarpsektorinius faktorius. Kaip pažymi E2 ekspertas: „Iš savo darbo patirties žiūriu ne vien tik organizaciją kaip tokią, vykdydami savo veiklą, žiūrime į atsparumą nacionaliniu valstybės lygiu, t.y. visą Lietuvos IP ruožą. Atsparumas, mūsų požiūriu, atsiremia į ryšio tinklus. Atsparumo sąvoka apima ne tik tinklų kibernetinį saugumą ir atsparumą kibernetinėms atakoms. Tinklų sistemos gali nukentėti ir nukenčia nuo žmogiškų klaidų, nuo elektros tiekimo sutrikdymų, kas tokiu atveju yra visiškai kito sektoriaus įtaka, nes jeigu elektra neteikiama ryšio tinklams, pastotė sustoja, iš nepertraukiamų maitinimo šaltinių ir generatorių neilgai gali tinklas veikti [...]“ (E2, asmeninis interviu, 2017 m. liepos 14 d.).
2. Kibernetinio atsparumo suvokimas per bendrą visų sociotechninės organizacinės sistemos komponentų gebėjimą pasipriešinti nepageidaujamam išoriniam poveikiui išlaikyti veiklos parametrus ir atstatyti veiklą po įprastinių nedidelio masto kibernetinių incidentų bei nenumatytų didesnio masto kibernetinių situacijų (katastrofų). „Organizacijos kibernetinis atsparumas - tai yra jos savybė ar

capability – gebėjimas, atsispirti išoriniam poveikiui, kibernetinės erdvės. Tai yra išlaikyti savo veiklą, pagrindinius veiklos parametrus, t.y.: 'darykit mums ką norit, o mums visiškai vienodai'. Tai – gebėjimas išlaikyti parametrus sukrėtimo ar nuolatinio kratymo atveju." (E4, asmeninis interviu, 2017 m. liepos 24 d.); „Galimybę organizacijai [*priešintis – aut.*], nes vien tik tinklas, kompiuterinis tinklas tai nėra, negalima taip išskirti, vis tiek aš galvočiau, kad tai yra organizacija. Atsparumas – tai pačios organizacijos galimybė priešintis atakoms arba greitai atstatyti savo veiklą įvykus kažkokiems incidentams, nebūtinai netgi atakoms. Ta prasme, galimybė pasipriešinti ir grįžti prie normalios būklės po kažkokių incidentų." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Pažymėtina, kad toks suvokimas yra pats artimiausias anglosaksiškose šalyse vyraujantiems atsparumo modeliams.

3. Kibernetinio atsparumo suvokimas per incidentų prevenciją bei pasirengimą jiems, taip pat kibernetinio atsparumo objekto gebėjimą išvengti krizinių situacijų visų organizacijos procesų kontekste, akcentuojant žmogiškųjų ir technologinių sistemų komponentų sąveiką, tačiau lemiamą vaidmenį skiriant žmogiškajam sociotechninės sistemos komponentui. „Kibernetinis atsparumas, būtų visuma pasirengimo tiek informacinių sistemų, tiek jas aptarnaujančių žmonių pasirengimo atremti ir išvengti kibernetinių incidentų [...], visuma teisinių, organizacinių ir IT priemonių, skirtų incidentams išvengti ir sistemų veiklai atstatyti. Vadinasi, parengtis prevencine prasme ir parengtis atakų prasme." (E5, asmeninis interviu, 2017 m. liepos 24 d.); „Atsparumo sąvoka – tai atsparus kibernetinėms atakoms, t.y realiai net nepadarant žalos tiek organizacijai, tiek ir kitiems tinklams […] arba [*leidžiantis – aut.*] jos išvis išvengti. Nes pagrinde yra, kad visas atsparumas ir visas saugumas susideda iš dviejų dalių: iš technologijos ir žmogaus, o žmogus realiai ir kuria tą technologiją. Tai iš esmės yra žmogus visą laiką [...]" (E6, asmeninis interviu, 2017 m. liepos 26 d.); „[...] viskas didžiąja dalimi priklauso nuo personalo, kuris yra atsakingas už minėtas įrangas. Tai, kaip personalas moka dirbti su šia įranga, yra tiesiogiai susiję su atsparumu, kibernetinio saugumo atsparumu [...]" (E3, asmeninis interviu, 2017 m. liepos 21 d.).

Plėtojant kibernetinio atsparumo sąvoką organizacinio atsparumo plotmėje, kibernetiniams incidentams atsparią organizaciją E1 ekspertas apibrėžė kaip taikančią prevencinius mechanizmus, leidžiančius jai sumažinti kibernetinių incidentų metu patiriamą žalą ir įgyvendinančią pasirengimo kibernetinėms grėsmėms bei incidentams skirtingose organizacijos veiklos plotmėse priemones: „Tai tiek techninėmis, tiek organizacinėmis priemonėmis pasiruošusi institucija (įmonė), kuriai maksimaliai sumažinta grėsmė patirti žalą arba kibernetinį incidentą, jei išskirti [*priemones – aut.*]: teisinės, organizacinės ir techninės." (E1, asmeninis interviu, 2017 m. liepos 11 d.). Vertinant šios interviu dalies rezultatus, pažymėtina, kad daugumos apklaustų ekspertų įvardintiems kibernetinio atsparumo apibrėžimams bei išskirtiems kibernetinį atsparumą formuojantiems elementams, ko gero, nemažą įtaką turėjo ir asmeninė ekspertų patirtis, veiklos profilis bei priklausymas konkrečią veiklą vykdančioms organizacijoms. Todėl bandant suvokti ir apibrėžti tam tikros ekspertų bendruomenės dalies naudojamas sąvokas, vertėtų įvertinti ir tokį faktorių kaip profesinis šališkumas.

Kibernetinio atsparumo sąvokų pozicionavimas bendroje kibernetinio saugumo terminų ontologijoje. IT industrija, kuri visuomet buvo ganėtinai dinamiška, yra pakankamai garsi ir dėl joje naudojamų sąvokų kaitos ir įvairovės bei situacijų, kai, esant senai nusistovėjusioms veiklos kryptims ir technologiniams modeliams, atsiranda naujos tendencijos, požiūriai bei nauji senų reiškinių pritaikymo metodai. Viskas kinta taip dažnai, kad paskui šiuos terminijos pokyčius nespėja keistis akademinė leidyba, sudėtinga visus šiuos dinamiškus procesus atspindėti ir teisės aktuose. Taip pat darosi sunku suprasti, kas yra naujas reikšmingas konceptas, o kas tiesiog marketinginės kampanijos metu sugalvotas „protingas žodelis“ (angl. *buzzword*), kurio atsiradimas sąlygotas siekiant parduoti senus produktus kaip naują prekę. Pagal E2 ir E7 ekspertus, šis dinamiškumas būdingas ir kibernetinio saugumo bei atsparumo sritims: „Šiuo metu visi naudoja skirtingas sąvokas, o kibernetinio saugumo srityje vykstantys procesai yra tiek dinamiški, kad sąvokos ir apibrėžimai tiesiog nespėja taip greitai keistis, kad realiai atspindėtų procesų esmę, kas sąlygoja tų pačių sąvokų dubliavimą bei skirtingų apibrėžimų vartoseną.“ (E2, asmeninis interviu, 2017 m. liepos 14 d.); „Anksčiau buvo: informacijos apsauga, paskui integralumas, prieinamumas, tokie terminai buvo: *information security* (informacijos saugumas), paskui *information assurance* (informacijos užtikrinimas).“ (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Taigi, kol vienose saugumo aplinkose vyksta diskusija apie bazinių sąvokų įtvirtinimą, kitose tuo metu bandoma įprasminti gan progresyvius požiūrius: „ES kibernetinio saugumo forumuose pasigirsta, iš tų pačių prancūzų atėjęs siūlymas naudoti terminą „elektroninis saugumas“ (*digital security*), nes tai yra plačiau nei „kibernetinis saugumas“ (*cyber security*). Tokie siūlymai, kokią terminiją naudoti yra diskusijų klausimas arba uždavinys tyrėjams [*nustatyti tinkamą terminiją – aut.*].“ (E2, asmeninis interviu, 2017 m. liepos 14 d.). Atsižvelgiant į visą reiškinio sudėtingumą, siekiant nustatyti konceptualų kibernetinio atsparumo pozicionavimą bendrame kibernetinio saugumo teoriniame lauke, interviu dalyvių buvo klausiama ar kibernetinis atsparumas turėtų būti integruojamas į egzistuojančią kibernetinio saugumo terminų topologiją, ar nagrinėjamas atskirai. Į ką ekspertai pateikė gan skirtingus atsakymus, tačiau dauguma jų pasisakė už kibernetinio atsparumo integraciją į egzistuojančią kibernetinio saugumo terminiją. Šiuos teiginius ypač gerai iliustruoja E7 eksperto nuomonė, kurio teigimu, kibernetinis atsparumas ir saugumas turėtų būti nagrinėjami bendrai todėl, kad kibernetiniam saugumui būdingos tarpdisciplininės, integruojančios savybės, apimančios žmogiškuosius ir techninius sistemos komponentus: „Žiūrint, kaip mes traktuojame kibernetinį atsparumą [...], ką mes laikome kibernetiniu saugumu – ar tai yra tik techninės priemonės? Man kibernetinis saugumas nėra tiktai geležis. Tai yra ir žmonių mokymas ir švietimas ir teisiniai (*legal*) aspektai, taisyklės. Jei laikyti kibernetinį saugumą tokiu – tai kibernetinis atsparumas [...]. Sakyčiau, kad čia beveik tas pats, lygybės ženklą dėčiau tarp jų. Jei žiūrėti kompleksiškai, o ne taip, kad: ‘nupirkom geležį ir viskas’. Sakyčiau, kibernetinis saugumas, plačiąja prasme, padengtų kibernetinį atsparumą.“ (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Būtent toks dviejų konceptų gimiringumas ir sąlygoja jų sanglaudą – tam tikra prasme, jie visuose kontekstuose turėtų būti pozicionuojami kartu. Dalies apklaustų ekspertų nuomone, svarbu šiuos du reiškinius vertinti bendroje perspektyvoje. Šį teiginį puikiai iliustruoja E1 eksperto nuomonė: „Jei išskiri viską atskirai, gali būti ir į jį bus pradėta žiūrėti atskirai.

Dėl to ir bus – saugumas sau, paslaugos sau. Todėl reikėtų įsivertinti. Kai kur gal ir galima išskirti į atskirus dalykus, tarkim politikos, strategijos.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Darytina prielaida, kad nors vieną nagrinėjamų reiškinių atskyrus, gali kilti rizika, kad šis konceptas iškris iš bendrojo saugumo konteksto ir iškils tokia pati grėsmė, su kuria susidūrė visos informacinės ir kibernetinio saugumo technologijos. Kai jos buvo vertinamos kaip visos organizacinės sistemos priedėlis, o ne kaip jos sudedamoji dalis, dėl ko neretai nukentėdavo jų finansavimas, arba tiesiog, vertinant bendruosius poreikius organizacijos veiklų visumoje, dažnai informacinių technologijų komponentai būdavo laikomi ne tokiais kritiniais, todėl nesulaukdavo pakankamo aukščiausios organizacijos vadovybės dėmesio. E2 ekspertas, papildydamas kibernetinio atsparumo sąvokų diskusiją siūlymais integruoti atsparumą į egzistuojančius kibernetinio saugumo teorinius modelius, pažymėjo, kad atsparumo integracija būtina dėl šio koncepto istorinių sąsajų su viena iš kibernetinio saugumo sudedamųjų dalių – tinklų atsparumu (angl. *network resilience*): „Vienareikšmiškai atsparumas turi būti integruotas į dabartines sistemas, nes istoriškai tai buvo tinklų atsparumas [...] – tai yra integrali viso kibernetinio arba elektroninio saugumo dalis ir negali būti atsieta.“ (E2, asmeninis interviu, 2017 m. liepos 14 d.).

Papildant kibernetinio atsparumo diskusiją kitų šalių pavyzdžiais, su E4 aptartas Prancūzijos atvejis, kai šios valstybės teisės aktuose buvo įtvirtintos alternatyvios anglosaksiškiems atsparumo modeliams kibernetinio tvirtumo savybės. Bandant nustatyti, ar tai, eksperto nuomone, būtų tinkamas modelis Lietuvai, pateiktas klausimas, ar vertėtų bandyti adaptuoti egzistuojančius kibernetinio atsparumo principus, ar vadovautis Prancūzijos pavyzdžiu ir bandyti ieškoti alternatyvių būdų. Siūlymas ieškoti alternatyvų eksperto buvo įvertintas skeptiškai. E4 manymu, tai reikalautų pernelyg didelių resursų, todėl reikėtų naudoti nusistovėjusią struktūrą ir bandyti naujai adaptuoti tik pačius būtiniausius terminus: „Ar sugebėsime ir, ar tikslinga įsivedinėti savo naują terminiją ir tą visa valdymo struktūrą? Abejočiau, manyčiau, kad ir išteklių turim ne tiek daug, kad tam skirti laiką. Efektyviausia būtų paimti jau veikiančią struktūrą ir keisti tik tai, kas būtina. Aišku, verčiant terminus į lietuvių kalbą [*pasitaiko – aut.*] ir nesusipratimų, ir nukrypimų, bet, manyčiau, kad tai sutvarkoma.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.). E3 eksperto nuomone, vertėtų atkreipti dėmesį, kad bandant adaptuoti vienai visuomenei ar visuomenės daliai priimtinus ir joje naudotinus terminus kitose aplinkose, gali kilti sunkumų: „Sąvokos yra naudojamos tokios, kurios yra suprantamos tai daliai visuomenės. Jei JAV naudojame *information assurance* [*sąvoka „informacijos užtikrinimas“ – aut.*], tai mūsų kalboje nėra analogiško vertimo. Kas yra *information assurance*? Taip, tiesiogiai, tai yra užtikrinimas, bet kas po juo slepiasi, apie ką mes kalbam? Ar mango yra sultys, ar vaisius, ar [...]? Kaip bepavadinsi, svarbu žinoti, apie ką mes kalbame, o sąvokos priklauso nuo visuomenės, kuri turi didesnį ar mažesnį kibernetinį raštingumą.“ (E3, asmeninis interviu, 2017 m. liepos 21 d.). Šie sunkumai gali rastis jau bandant konkrečius terminus išversti ir, kas svarbiausia, tinkamai suvokti. Taigi, tyrimo autorius pritaria E3 eksperto išsakytoms idėjoms, kad kibernetinio saugumo sąvokų teorinis gylis ir jų formavimo ypatumai priklauso nuo tam tikros visuomenės ar kritinės tos visuomenės dalies kibernetinio saugumo raštingumo. Taip pat buvo išsakytų nuomonių, siūlančių kibernetinį atsparumą apibrėžti kuo konkrečiau, nebandant jokių sąvokų konceptualiai sulieti tarpusavyje. Ypač tai akcentavo E5 ekspertas: „Aš už

tikslų sąvokų apibrėžimą. Tikrai negerai, kai vartojama kažkaip sinonimiškai ar konkuruojančiai viena su kita. Aš už tai, kad būtų ar standarto, ar įstatymo, ar poįstatyminio kokio nors vyriausybės nutarimo lygmeniu pagrindiniai šitie terminai, sąvokos, ypač susijusios su sauga, būtų apibrėžtos. Kad visi vienodai suprastų kas tai yra incidentas, kas yra atsparumas, kas yra kibernetinis saugumas – labai svarbu.“ (E5, asmeninis interviu, 2017 m. liepos 24 d.).

Kibernetinio atsparumo reglamentavimo būklės įvertinimas. Diskutuojant su ekspertais buvo bandoma įvertinti jų nuomonę apie tai, ar pakankamai atsparumas apibrėžtas LR teisės aktuose, ir jei ne – ką galima šioje srityje būtų tobulinti. Ekspertai pažymėjo, kad konkrečios atsparumo sąvokos dažniau sutinkamos ES ir NATO teisės aktuose: „Kibernetinio atsparumo, tai tokios sąvokos, bent jau aš nepamenu [*LR teisės aktuose – aut.*], bet europiniuose, NATO *cyber resilience* yra minimas. Apibrėžimą geriausiai galėtų pasiūlyti kibernetinio saugumo politiką formuojanti organizacija [...]. Tarp ES teisės aktų tas kibernetinis atsparumas – tai yra viena iš siekiamybių, šalia atgrasymo priemonių.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.). Tačiau, jei apie atsparumą vykdomos diskusijos valstybiniu lygmeniu, teisės aktuose, E1 eksperto nuomone, turėtų būti pateikiamas bent sąvokos apibrėžimas: „Jis turėtų būti bent jau plačiau, nes vienas sakinys yra kaip terminas. Ir turėtų būti plačiau paplėtotas kokiomis priemonėmis, principais – kas tą apima.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Tuo pačiu klausimu kai kurie ekspertai kelia kitą klausimą – ar būtinai reikalingi tam tikri atskiri, specializuoti atsparumo dokumentai: „Teisės aktuose dabar pas mus, kad to nėra išskirta tai faktas, kad išskirti galbūt reikėtų, gal ir nieko, bet ar jo dabar nėra visai?“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). E1 eksperto nuomone, galbūt Lietuvoje tos pačios ar gimininges atsparumo idėjos yra atspindimos per kitus dokumentus: „Tarkime, jei žiūrėti klausimas pažodžiui, kas yra atsparumo strategijoje. Gal pas mus tos pačios nuostatos atsiranda kažkur kituose dokumentuose, todėl nėra pats atsparumas išskiriamas.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Galbūt, pavyzdžiui, Škotijos, kuri turi kibernetiniam atsparumui dedikuotus dokumentus, kibernetinio atsparumo strategijoje esančios atsparumo nuostatos Lietuvos teisės aktuose realizuojamos kitais mechanizmais: „[...] reikia pasilyginti dokumentus, nes lygiai taip pat yra su kitais dokumentais, kur, tarkim, pas vienus yra atskiras įstatymas kibernetinio saugumo, pas kitus yra kitų penkių šešių ar septynių įstatymų dalys. Tai vat klausimas, ar verta čia turėti vieną ar skirtingose srityse tai segmentuoti.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Esant tokiai situacijai, labiausiai reikėtų akcentuoti, kaip tų mechanizmų visumos tarpusavio sąveikos potencialas gali padėti atsakyti į kylančius iššūkius, kuriuos analogiškose situacijose numatyta spręsti kitomis atsparumo plėtojimo įstatyminėmis priemonėmis: „Rengiam nacionalinius teisės aktus, žiūrim visumą, žiūrim incidentų šalinimo, sprendimo procesus, kur prasideda nuo detektavimo, tada analizės veikimo ir baigiasi – išmoktos pamokos, kad kitą kartą, tokiam incidentui atsitikus, atsistatymas būtų greitesnis.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.).

Egzistuojanti kibernetinio saugumo apibrėžimų problematika. Diskutuojant su ekspertais kibernetinio saugumo terminijos klausimais buvo įgyta nemažai ir su egzistuojančia kibernetinio saugumo ir jo sąvokų problematika susijusių įžvalgų, kurios atskleidė, kodėl dauguma tyrimo dalyvių yra linkę taikyti unifikuotas kibernetinio saugumo srities sąvokas

ir yra skeptiškai nusiteikę naujos terminijos plėtojimui. E5 ekspertas griežtai pasisakęs už tikslesnį kibernetinio atsparumo apibrėžimą, pastebėjo, kad šiuo metu Lietuvoje identifikuojamų saugos traktuočių skaičius yra pernelyg didelis: „Yra daugybė sąvokų, kur apskritai varijuoja, ko neturėtų būti – tai yra ta pati sauga. Dabar yra: valstybės informacinių išteklių sauga, kibernetinis saugumas, elektroninės informacijos sauga, informacinių technologijų sauga ir dar rastumėt saugų [...], informacinė sauga, ne informacijos ar karų informacinių, o IT saugos prasme, kažkodėl ūkio sektoriuje šita sąvoka." (E5, asmeninis interviu, 2017 m. liepos 24 d.). E4, priešingai, kaip neigiamą tendenciją pastebi egzistuojančią tam tikrą terminijos niveliaciją. E4 nuomone, šios saugos turėtų būti plėtojamos atskirai, o problema dabar yra tame, kad viską užgožia kibernetinis saugumas, eksperto nuomone, tuomet lieka vienalypis šabloninis konstruktas, o tokia padėtis trukdo įvairiapusiam reiškinio supratimui ir atskirų saugos veiklų plėtojimui: „Faktiškai kibernetinis saugumas pakeitė visą terminologiją, va tą informacijos apsaugą, visas jos sritis. Ir IT apsaugą, tos visos veiklos sritys nuėjo į antrą planą. Pirmoje eilėje yra kibernetinis saugumas. Tai visa kompiuterinė sauga, ar informacijos – viskas yra po tuo skėčiu. Nors iš teorinės pusės, tai gal ir nėra gerai. Tai daugiau technologinė sauga, šalia jos – organizacinė sauga, dar yra fizinė sauga, tai, kas nepapuola į kibernetinio saugumo sritį pagal nutylėjimą. Tos sritys užgožiamos." (E4, asmeninis interviu, 2017 m. liepos 24 d.). Tačiau, analizuojant praktinius pavyzdžius kibernetinio saugumo sektoriaus pertvarkos kontekste, kai vienos institucijos iš kitų perima kibernetinį saugumą kaip valdymo sritį, E5 eksperto manymu, yra akivaizdu, kad pernelyg didelis skaičius panašių sąvokų gali būti pakankamai didelis trukdis tinkamam kibernetinio saugumo valdymo uždavinių įgyvendinimui: „Visuomet jei deriname teisės aktus, siūlome suvienodinti ir siūlome versiją, kuri geriausia. Dabar susidūrė su problema KAM, nori perimti šią sritį iš VRM – sunkiai sekasi apibrėžti kokio platumo ta sritis, kuri yra pavaldi VRM. Nes štai išteklių sauga pagal įstatymą, el. informacijos sauga po klaustuku pagal Vyriausybės nutarimą, vėlgi ta informacinė sauga pagal nacionaliniam saugumui svarbių įmonių ir įrenginių įstatymą – ten staiga išlenda informacinė sauga, tų įmonių, kurios įtrauktos į svarbių nacionalinio saugumo sąrašą. Painiavos čia nemažai. Dabartinis kibernetinio saugumo apibrėžimas visiškai apeina šitą branduolį kibernetinio saugumo." (E5, asmeninis interviu, 2017 m. liepos 24 d.). Vertinant situaciją su daugybe saugų akcentavimu, darytina išvada, kad saugos terminija nejuda gilesnio srities suvokimo link per bandymą apibrėžti ir gilintis į gretutines saugumo sritis, tačiau plėtojimas vykdomas horizontaliame lygmenyje formuojant įvairių gretutinių veiklos sričių informacinio saugumo principus. Apibendrinant ekspertų įžvalgas, pažymėtina, kad viskas atsiremia į organizacijos narių kibernetinį raštingumą tiesiogiai ir į bendrą srities diskurso plėtotės lygį konkrečioje kibernetinio saugumo sistemoje. Kuo didesnis kibernetinis raštingumas vyrauja joje, tuo tikslesnės sąvokos taikomos, bandant detalizuoti tam tikrus reiškinius ir nagrinėti juos giliau. Bendras šių tikslių sąvokų skaičius gali būti mažesnis, tačiau jos yra ypač tikslios, taigi visų sistemos dalyvių suvokiamos pakankamai vienodai. Tai visiškai priešinga padėčiai, kai nepasiektas tam tikras kibernetinio atsparumo suvokimo brandos lygis, egzistuoja tam tikras atsparumo ar saugumo diskursas, tačiau kai nėra išgryninti, suvienodinti ir apibrėžti elementarūs dalykai, darosi sunku pereiti prie sudėtingesnių konceptų, tokių kaip užtikrinimas (angl. *assurance*), atsparumas (angl. *resilience*) ir pan., aptarimo.

3.1.1. Kibernetinio atsparumo didinimui didžiausią įtaką turintys veiksniai

Su ekspertais diskutuojant apie galimybes padidinti kibernetinį atsparumą, į klausimą kokie komponentai, veiksmai, instituciniai pokyčiai ar procesų pakeitimai ir kitokios priemonės leistų padidinti organizacijų kibernetinį atsparumą, apklausti ekspertai pateikė gana skirtingus siūlymus, pradedant orientuotais į konkrečius technologinius aspektus: „Galima atsparumą stiprinti tinkluose atskirai, darant rezervines linijas, atsargines kopijas tam, kad sistema būtų diversifikuota ir atspari krizėms ir didelio masto kibernetinėms atakoms." (E2, asmeninis interviu, 2017 m. liepos 14 d.) bei siūlymus spręsti valstybės IT sistemų komponentų suderinamumą: „Su kokiu rūpesčiu susiduria VT institucijos – vadinamu zoologijos sodu, tai yra įvairiausiais, kartais nesuderinamais tarpusavyje IT sprendimais. Finansavimas, kaip taisyklė, skiriamas jų atnaujinimams, o man atrodo, kad atsparumą didintų naujas sprendimas, apimantis visumą. Ne fragmentus atnaujinti ir taisyti, o pagalvoti apie bendrą naują sprendimą." (E5, asmeninis interviu, 2017 m. liepos 24 d.), baigiant personalo ir, kas ypač svarbu – sistemų naudotojų gebėjimais: „Personalo gebėjimai labai svarbūs. Ir ne tik IT personalo, bet naudotojų, jų gebėjimų ugdymas, nes šiuo metu žmogus yra silpniausia grandis. Aišku naujausių IT sprendimų diegimas." (E5, asmeninis interviu, 2017 m. liepos 24 d.); „Per mano praktiką, tai yra susiję su keliais tokiais pagrindiniais aspektais: visų pirma, žmogaus gebėjimai, čia galime sutapatinti ir privatų sektorių, ir valstybinį." (E3, asmeninis interviu, 2017 m. liepos 21 d.). E1 ekspertas akcentavo individualų požiūrį kiekvienos institucijos atveju bei adekvačių saugos priemonių taikymą, tačiau visoms institucijoms būtinu veiksniu įvardino rizikų vertinimą: „Tai kiekvienos institucijos reikalas, kuri, mažų mažiausiai, turi pradėti nuo rizikų vertinimo, įsivertinti per kur gali patirti atakas, žalą, kad parinkti atitinkamas technines rizikos mažinimo priemones. Saugotų tą vietą, per kur jiems skaudžiausia, kad nebūtų taip, kad saugo savo perimetrą, o jiems tas realiai visai neaktualu, nes, pavyzdžiui, jų informacija yra *debesyje*. Dėl to ir yra rizikos vertinimai. Galbūt vienai įmonei prastova dienos ar valandos, kai jie bus atakuojami, nebus tokia skaudi, kaip kas metus mokėti po didelę pinigų sumą už tam tikrą produktą, kurio galbūt jiems nereikės – tai irgi atsiremia į rizikos vertinimą." (E1, asmeninis interviu, 2017 m. liepos 11 d.). Kaip vieną esminių techninių proaktyvių priemonių E2 ekspertas išskyrė įsilaužimo galimybės įvertinimų (angl. *penetration testing*) svarbą ir efektyvumą: „Akcentuoti reikėtų *penetration testing* [*įsilaužimo galimybės įvertinimus – aut.*]. *Penetration* testai yra saugumo audito dalis ir yra labai pasiteisinę ir visi rekomenduoja kuo daugiau tuo naudotis. Tu gali nusimatyti, inventorizuotis, kategorizuotis, įsivaizduoti savo labiausiai jautrias sistemas, bet visko gali nenumatyti ir tada *penetration* testai gali atskleisti silpnąsias vietas, tada tu jas gali užlopyti ir, tokiu būdu, sustiprinti atsparumą. **Tad akcentą dėčiau ant penetration testų kaip labai efektyvaus įrankio didinti atsparumą."** (E2, asmeninis interviu, 2017 m. liepos 14 d.). Plėtojant diskusiją apie žmogiškųjų gebėjimų vaidmenį kibernetinio atsparumo užtikrinimo procesuose, E3 ekspertas kritiškai pastebėjo, kad dažnai šie gebėjimai ir darbuotojų kompetencijos nėra tikrinamos ir tinkamai įvertinamos, taikomas pernelyg formalus požiūris: „Niekas netikrina jo gebėjimų. Jo norai, išsilavinimai gali būti bet kokie, bet ar jis geba atlikti tą darbą – neįdomu. Kodėl netikrina? Galbūt todėl, kad niekas nesupranta esmės klausimo – kodėl turėtų tikrinti, jis turi diplomą, sako, kad moka

daryti, pasodini prie įrangos, jis kažką paspaudo, kažkas gaunasi, bet ar jis sugeba laiku ateiti į darbą, jis galvoja nuo pietų, kaip išeiti iš darbo, jam nesvarbu kokie procesai naktį dedasi. Tai čia jau turi būti asmeninės savybės.“ (E3, asmeninis interviu, 2017 m. liepos 21 d.). E3 eksperto nuomone, šioje srityje galėtų turėti pozityvių implikacijų darbuotojų motyvacijos gerinimas ir jo vykdomos veiklos svarbos suvokimo didinimas: „Su motyvacija yra daug paprasčiau, ji išskaičiuojama matematiškai: visų pirma – pinigai, antra – garbė, trečia – noras tobulėti ir sėdėti viršūnėje. Tarp visų motyvacijos elementų yra ir iššūkiai. Tai vat, visuma šitų klausimų turėtų atsakyti kodėl nėra [atsparumo – *aut.*]. Viskas pradeda suktis, kai yra visi keturi aspektai viename ir jų suma duoda aukščiausią balą. Kai žmogus patenkintas, laimingas, motyvuotas jis gali prisiliesti prie naujausių technologijų pavaldyti, pasukioti palydovą [...], užtai jam nereikia galvoti ką vakare valgyti. Jis yra pareigingas ir supranta, ką jis daro ir kaip tai yra svarbu kitiems aplinkiniams susijusiems procesams, žmonėms, kompanijoms ir t.t.“ (E3, asmeninis interviu, 2017 m. liepos 21 d.). E3 eksperto manymu, atliekamo darbo svarbos suvokimas bei tobulėjimo galimybių matymas formuoja pagrindą asmeninio, o vėliau organizacinio atsparumo formavimui. E6 ekspertas, kalbėdamas apie žmogiškąjį faktorių kibernetinio saugumo ir atsparumo gerinimo kontekste be pastebėjimo, kad saugumo finansavimas yra nepakankamas, atkreipė dėmesį, kad trūksta švietimo kibernetinio saugumo srityje ir apskritai kibernetinio raštingumo, o ypač, eksperto nuomone, tai aktualu kalbant apie vyresnio amžiaus darbuotojus: „Mažai investuoja įmonės. Trūksta ir sampratos ir švietimo, ir ta dalis žmonių, kurie yra virš 50 metų, tai dažniausiai finansininkai, buhalterės ir pan. labai jautrūs yra, nes jie su kompiuteriu neužaugo. Tas ceo fišingas, tos atakos kai apsimeta direktoriumi yra labai sėkmingos, o įmonei yra labai skausmingos. Paprasčiausiai priežastis – nėra švietimo, jos nežino, nepatogi situacija, o kitas yra technologinė – nenaudoja pašto apsaugos priemonių.“ (E6, asmeninis interviu, 2017 m. liepos 26 d.). Taip pat vertėtų pažymėti , kad vykstant masinei organizacijų kompiuterizacijai, dažnai buvo keliamas klausimas apie vyresniojo amžiaus darbuotojų atskirtį dėl nepakankamo jų kompiuterinio raštingumo. Ilgainiui, gerėjant šiai demografinei grupei priklausančių darbuotojų kompiuterinei kompetencijai, šios diskusijos nutilo, tačiau panašu, kad šis klausimas gali vėl atsidurti suinteresuotų šalių dienotvarkėje, tačiau jau ne dėl bendrojo kompiuterinio, o dėl kibernetinio saugumo raštingumo. Švietimo svarbą, kartu su tinkamu reglamentavimu ir pasirengimu bei planavimu akcentavo ir E1 ekspertas: „Labai svarbus darbuotojų švietimas: tiek bazinis žinių pakėlimas, tiek tam tikrų administratorių gilesnis mokymas. Pats pasiruošimas, jeigu turi kažkokį testavimo, veiklos tęstinumo planą, informacinių sistemų atstatymo planus, turi pasirengęs visų komunikacijų planus, kaip komunikuoti, ką transliuoti visuomenei ar klientams. Kaip visų grandžių specialistai dirba: pradedant administratoriais, baigiant vadovais. Tokį planą veikimo turėsi, kaip reikalauja geroji praktika, kaip reikalauja nacionaliniai teisės aktai, tai tavo atsistatymas į pradinę būseną bus daug greitesnis.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). E1 manymu, kalbant apie tinkamą žmogiškųjų resursų valdymą, stiprinant organizacijų kibernetinį atsparumą – ypač svarbus faktorius yra ir reglamentavimas: „Lygiai tas pats – organizaciniai dalykai – viskas turėtų būti reglamentuota, kad darbuotojai dirbtų pagal procesus, kad žinotų, kada reikia kur kreiptis, kada reikia ką daryti.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Kalbant apie valstybės tarnautojų kibernetinį

švietimą, vertėtų išskirti, jog atliekant interviu vis pasigirsdavo ekspertų siūlymų, kad kartu su įprastiniais valstybės tarnybos įvadiniais mokymais, būtų naudinga padaryti privalomus kibernetinio saugumo pagrindų mokymus valstybės tarnautojams. E6 eksperto siūlymu, tokie mokymai turėtų būti organizuojami reguliariai, o kaip gerosios praktikos pavyzdį ekspertas pateikė vienoje JAV valstijoje vykdomus reguliarius darbuotojų kibernetinio saugumo žinių testavimus bei kaip teigiamą dalyką pažymėjo, kad tokie žingsniai jau po truputi daromi ir Lietuvoje: „Reikia dažniausiai naudojamus [*klausimus – aut.*], bet jis turi būt nuolatinis, jei jis kaip įvadinis mokymas, tai aš jo neatsimenu. Labai gera praktika, pavyzdžiui, Jutos valstija JAV daro visam valstybiniam sektoriui testą. Pradžioje supažindina su kibernetinėmis atakomis, o paskui daro testą ir tu turi jas atpažinti, *online* forma. Privalo visi valstybinės institucijos darbuotojai jį praeiti, senatoriai. [...] Man atrodo estai yra kažką panašaus sukūrę. Lietuviai irgi bando kažką padaryti, mes nedalyvaujame, kita ministerija dalyvauja. Tas yra labai gerai valstybiniame sektoriuje – atpažinti ir identifikuoti [*kibernetines grėsmes – aut.*].“ (E6, asmeninis interviu, 2017 m. liepos 26 d.). E5 eksperto manymu, valstybės tarnyboje turėtų būti privalomas įvadinis kibernetinio saugumo kursas: „Aš padaryčiau privalomą kursą valstybės tarnyboje, tarnautojams, darbuotojams dirbantiems pagal darbo sutartis. Kaip būna tie įžanginiai valstybės tarnybos kursai, aš būtinai įtraukčiau moduli paprasčiausios saugos, higienos IT srities.“ (E5, asmeninis interviu, 2017 m. liepos 24 d.). E7 ekspertas taip pat akcentavo tinkamą kibernetinio saugumo reglamentavimą, saugumo kultūros ugdymą bei valdančiosios grandies požiūrio į egzistuojančias kibernetinio saugumo problemas kaitą ir šio požiūrio sklaidą organizacinės hierarchijos vertikale iš viršaus žemyn: „Visų pirma, reglamentavimas, taisyklės teisės aktai vidiniai – čia gal net ne pirmas dalykas būtų. Pirmas tai būtų – valdžios mąstymo pasikeitimas. Dažniausiai yra visose įstaigose, kol nesusiduria su problema, tol vadovas galvoja, kad tos problemos nėra. Tai vat, pradžioj vadovo mąstymo pasikeitimas, tada to mąstymo perdavimas darbuotojams ir tada reglamentavimas teisės aktais, taisyklėmis, tvarkomis kompiuterių, programinės įrangos naudojimo. Požiūrio į kibernetinį saugumą keitimas ir kultūros ugdymas.“ (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). E5 ekspertas pastebėjo, kad ypač svarbūs faktoriai gerinant organizacijų kibernetinį atsparumą yra bendradarbiavimo gerinimas, kibernetinių incidentų sprendimas vieno langelio principu, didesnė institucijų koordinacija bei aiškus veiklų pasidalijimas, padedantis išvengti jų dubliavimo: „Dabar CERT'ų yra ne vienas, RRT CERT'as, KSC CERT'as. Valstybinio sektoriaus atžvilgiu jie dubliuoja vienas kitą. Problema su informavimu, apie incidentus informuoti reikia abu šituos CERT'us, maža to, jei susiję su asmens duomenimis – dar ir Asmens duomenų apsaugos inspekciją. Jeigu turi nusikaltimų požymių – ir policiją. Gerai būtų vieno langelio principu valdyti incidentus. Tai yra apjungti kažkaip, jei ne institucijas, tai bent jau kažką priskirti tokį operacinio pobūdžio, kad kreiptis institucijoms valdant incidentus tektų į vieną organizaciją, o ji savo ruožtu, pavyzdžiui, nukreiptų į policiją, jeigu reikia. Šita prasme, bendradarbiavimas būtų gerai, taip pat ir koordinavimas.“ (E5, asmeninis interviu, 2017 m. liepos 24 d.). E4 ekspertas, kaip kibernetinio atsparumo tobulinimo priemonę pasiūlė visa apimančio kibernetinio saugumo požiūrio taikymą ir adekvačių priemonių formavimą pagal esamas grėsmes: „Kibernetinio atsparumo srity organizacijoms riekia žiūrėti ir į visumą. Atsparumas susijęs su tuo, kiek geras esam taikinys. Kiek

mes esam vertingi tam puolėjui, kuris mus puls ir atitinkamai mes turėtume ir planuoti savo „tvoras“ kibernetines, kad pas mus neįliptų.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.). Paklaustas apie institucinės sąrangos pokyčių galimą poveikį atsparumui E1 ekspertas pažymėjo, kad šios priemonės turėtų būti vertinamos kiekvienos institucijos atveju individualiai: „Institucija nelygu institucijai, bet faktas, kad už saugumą turi būti kažkas atsakingas, ar padalinys, ar žmogus, pagal visus nacionalinius dokumentus, kurie dabar yra, turi būti atsakingi už sistemas: saugos vadovas, administratorius.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Plėtodamas diskusiją apie kibernetinio saugumo reglamentavimo būtinybę E1 ekspertas pastebėjo, kad tinkamas reglamentavimas ypač svarbus esant krizinėms situacijoms ir gali pasitarnauti kaip saugiklis, kai kyla panika, tačiau esant aiškiai apibrėžtiems procesams, visi darbuotojai žino savo funkcijas ir tinkamai vykdo jiems pavestas pareigas: „Priklausomai nuo atakos, nuo grėsmės, nuo masto – vienu atveju gali būti mažesnis, kitų atveju didesnis laiko tarpas per kurį tu atsistatai, bet viskas susiveda į tai, kad kai kažkas atsitinka, dažniausiai pas žmogų mąstymas „išsijungia“, todėl jei bus kažkur kažkas surašyta kaip reik elgtis.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). E7 ekspertas pabrėžė sisteminio požiūrio į kibernetinį saugumą poreikį bei vertinimo lygiagrečiai su kitomis veiklos sritimis būtinybę: „Sisteminis požiūris į kibernetinį saugumą organizacijoje – kaip į bet kurią verslo sritį. Kibernetiniam saugumui, technologijoms, atsparumui reikia skirti pakankamai dėmesio, galbūt net kaip ir renkantis direktorių įmonės arba sudarinėjant biudžetą, arba sudarinėjant planą organizacijos veiklai metams. Galvojant apie ateities viziją taip pat reikia ir apie kibernetinį saugumą galvoti. Nes kitaip gaunasi, jeigu tu viską darai *ad hoc*, kad tu pribėgai: ‘va čia vat reik padaryti – užgesinau gaisrą ir toliau neturiu jokio plano ką aš darysiu’. Tai net negalima ir šnekėti apie tą kibernetinį saugumą. Nelaikyti kaip skylių lopymo, taikyti sisteminį požiūrį ir tai turi būti lygiavertė veikla su visom.“ (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Vienu iš gretutinių šios interviu dalies klausimų ekspertams buvo: ar galėtų atsparumo tobulinimas įtakoti viešojo sektoriaus organizacijų evoliuciją. E7 ekspertas atsakydamas į šį klausimą teigimai, pažymėjo, kad tai yra natūralūs procesai, nes vykstant atsparumo tobulinimui, lavinami darbuotojai, gerinamas jų ir vadovų situacijos suvokimas, kinta požiūriai į saugumo problematiką: „Kitaip ir būti negali, jeigu tu didini atsparumą pačioje organizacijoje – keisti, lavinti žmones, požiūri darbuotojų, kurie atsakingi. Vadovai galų gale pradeda suprasti, mąstyti apie tą kibernetinį saugumą ir pradeda tada pati kartelė [*kilti – aut.*], supratimas auga. Vadovas perduoda paskui pavaldiniams ir visa organizacija tobulėja, juda į viršų.“ (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). E1 ekspertui diskusijos eigoje buvo užduotas klausimas, ar kibernetinio atsparumo sąlygojama valstybinių institucijų saugos sistemų evoliucija galėtų kaip nors sukurti papildomą vertę piliečiams. Į ką ekspertas išsakė nuomonę, kad, jo manymu, sąsajų su verte gal ir nėra, tačiau pakankamai glaudžių ryšių galima įžvelgti tarp kibernetinio saugumo sistemų vystymo ir piliečių pasitikėjimo valstybinėmis institucijomis didėjimo: „Vertę gal ne, bet pasitikėjimą daugiau. Visi piliečiai žino, kad mūsų duomenys apdorojami tiek VMI, tiek SODR’os, bet jei aš rūpinuosi savo duomenimis, man svarbu, kad tos įmonės, kurios apdoroja, kad ten būtų viskas saugu. Kaip rodo, pavyzdžiui, VRK, kai buvo atskleisti duomenys, realiai rinkėjo duomenys – gyvenama vieta, adresas, asmens kodas. Tuos duomenis norint – gali panaudoti. Taip ir kilo tas

nepasitenkinimas. Kaip bebūtų, jei patirs žalą, tas vėl eis į viešumą, kris institucijų reputacija – kas paveiks ne tik institucijos vadovą, bet ir bendrai piliečių pasitikėjimą valstybe. Galų gale tai gali ir riaušes sukelti, suirutes – negali žinoti." (E1, asmeninis interviu, 2017 m. liepos 11 d.). E4 paklaustas, ar per atsparumo situacijos žinomumo bei atsparumo bendradarbiavimo mechanizmų gerinimą galima tobulinti viešojo sektoriaus kibernetinio saugumo valdymą ir taip šioje srityje prisidėti prie viso viešojo sektoriaus evoliucijos, pažymėjo, kad būtent šie išvardinti faktoriai padėjo tobulėti Estijos kibernetinio saugumo sistemai – tai ir yra būtent tos savybės, kurių stokoja Lietuvos viešasis sektorius, t.y. bendradarbiavimo ir savanoriškumo kultūros: „Kodėl estai mus aplenkė ir pabėgo? Todėl, kad pas juos tokia kultūra, pas juos bendradarbiavimo kultūra, savanoriškumo kultūra – pas mus trūksta tokios kultūros. Gal tai ir yra ta priežastis, kad kiekvienas savo kampelyje užsidaręs. Kol nieko neliečia, tai vat ir sėdi." (E4, asmeninis interviu, 2017 m. liepos 24 d.).

3.1.2. Organizacijų kibernetinio atsparumo didinimo iššūkiai

Kalbėdami apie dabartinę bendrą kibernetinio saugumo bei atsparumo situaciją Lietuvoje, dalis ekspertų pastebėjo, kad pastaruoju metu ji akivaizdžiai gerėja ir, kaip pažymėjo E6 ekspertas, tas gerėjimas vyksta ne tik konkrečiose institucijos, bet ir vertinant bendrai iš kibernetinio saugumo strateginių plėtros perspektyvų: „Situacija, bendrai atsparumas tikrai gerėja, aš jau 10 metų dirbu šitoje srityje ir matosi, kad samprata saugumo ir svarba tikrai didėja. Yra kai kurie atvejai, kur *Petyos*, *Wannacry* dideles įmones, korporacijas užvaldė, bet išmokstamos pamokos ir vis daugiau ir daugiau įmonių apsisaugo. Ir strateginis [*teigiamas pokytis – aut.*] yra, tuo pačiu ir rengiama kibernetinio saugumo strategija, kuri šnekės apie švietimą organizacijose." (E6, asmeninis interviu, 2017 m. liepos 26 d.). E5 ekspertas kaip pozityvų pokytį akcentavo, kad vykdomos diskusijos apie egzistuojančias problemas ir pažymėjo didesnį skirtingų organizacijų įsitraukimą, tačiau pastebėjo, kad įstatyminė bazė turėtų būti tobulinama: „Problemos įvardintos, net sakyčiau ant bangos, net kelios organizacijos taip aktyviai ėmėsi šitų procesų. Įstatymą reikėtų tobulinti, mano požiūriu, kibernetinio saugumo." (E5, asmeninis interviu, 2017 m. liepos 24 d.). E5 ekspertas taip pat pastebėjo, kad padėtį pagerino kibernetinio saugumo valdymo centralizacija ir jo sutelkimas vienoje institucijoje: „Dar vienas teigiamas dalykas – tai IS, registrų saugą sukoncentruos KAM vienose rankose. Nebus to neaiškumo, kad už valstybės informacinių išteklių saugos politiką atsako VRM, už kibernetinio saugumo politiką, įskaitant valstybės informacinių išteklių KAM. Aš negaliu logiškai atskirti, kuo kibernetinis saugumas skiriasi nuo išteklių saugos. KAM turi gerų idėjų visą saugą, kibernetinį saugumą plius išteklių saugą suimti į vienas rankas. Maža to – ir apjungti į vieną savo padalinį ir sistemų ir tinklų, kuriais apdorojama įslaptinta informacija, saugą. Vadinasi nepriklausomai, ar tai bus sistema skirta bendrai informacijai, ar įslaptintai ir nesvarbu, kokiu pjūviu – ar sauga ir saugos politika, ar kibernetinis saugumas – bus jau viena atsakinga institucija, manau, kad tai geras žingsnis ir tendencija." (E5, asmeninis interviu, 2017 m. liepos 24 d.). Kalbėdamas apie egzistuojančias problemas E1 ekspertas išskyrė nepakankamą dėmesį saugumo sričiai ir jos įtrauktį į bendrus organizacijos procesus ir pastebėjo, kad tai turi būti sprendžiama teisės aktų pagalba, kurie apibrėžtų kaip kibernetinio saugumo aspektai turėtų būti

inkorporuoti bendrame organizacijos veiklos kontekste: „Dėl to tas ir turi atsirasti, apie ką mes kalbėjome kokiais 2011 m. Ir atsirado veiklos plane 11–19 metais (Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa), kad turi atsirasti normali rizikų vertinimų metodika, grėsmių vertinimo metodikos, kad valstybės institucijos gebėtų surišti savo veiklos funkcijas su IT, modernizuoti procesą ir inkorporuoti saugumo aspektą, kad užtikrinti teikiamos paslaugos kokybę. Minėta programa yra strateginis dokumentas, jame buvo nuostatos dėl tam tikrų dalykų atsiradimo, bet arba aš jų nežinau, arba jie neatsirado." (E1, asmeninis interviu, 2017 m. liepos 11 d.). E4 pažymėjo, kad visgi nėra pakankamai gerai išgrynintas atsparumo konceptas ir viso kibernetinio saugumo sektoriaus problematika ir abiejų reiškinių (kibernetinio saugumo) atsparumo objektai: „Na tai pirmoji spraga, ne spraga, o tiesiog kai objektas, apie kurį kalbama nėra išgrynintas ir užakcentuotas, kad tai yra tai, į ką reikėtų kreipti dėmesį. Žodžiu, atsparumas – tai yra dalis bendros problematikos ir ji ta visa problematika nėra jau taip išgryninta, tai yra kalbama apie kibernetinį saugumą apskritai ir kas jį sudaro, tai kyla daug klausimų, tai yra kuo reikėtų pasirūpinti, į ką reikėtų atsižvelgti kiekviena sritis turi savo specifiką ir taip į jas gilintis reikia." (E4, asmeninis interviu, 2017 m. liepos 24 d.). E5 ekspertas gan kritiškai atsiliepė apie augančių rolių skaičių dabartinėse kibernetinio saugumo valdymo struktūrose, neaiškų jų tarpusavio santykį ir neapibrėžtus vaidmenis – kaip konkrečiomis priemonėmis šios rolės galėtų prisidėti prie atsparumo didinimo: „Organizaciniai dalykai gal ir neblogai sutvarkyti, bet kritiškai žiūriu į daugėjančias atsakomybes, kaip dabar yra trys net: saugos įgaliotinis yra asmuo, atsakingas už kibernetinį saugumą arba kibernetinio saugumo vadovu jis vadinamas. Ir atsiras dar vienas naujas asmuo, sulyg įsigaliojusiu asmens duomenų saugos reglamentu – tai asmuo, atsakingas už asmens duomenų saugą, ar vadinamas asmens duomenų saugos pareigūnas. Tai vat, rolių daug, santykiai nelabai aiškūs tarp jų. Ar tai ta pati pareigybė vėl neaišku. Bet, visi šie pareigūnai yra politikos formavimo ir priežiūros, negu kad realiai dirbantys ir didinantys kibernetinį atsparumą." (E5, asmeninis interviu, 2017 m. liepos 24 d.). Šiuos teiginius patvirtina ir E4 eksperto išsakytos įžvalgos. Paprašytas pakomentuoti saugos įgaliotinio rolės svarbą ir vaidmenį dabartiniame atsparumo plėtros kontekste E4 pažymėjo, kad ji deja jau neturi tiek įtakos, kiek informacinės saugos formavimo pradiniuose etapuose: „Idealiu atveju – taip, bet deja realybėje turim, kad, prieš atsirandant kibernetiniam saugumui, tos srities aktualumas tiek pakrito ir saugos įgaliotiniai neturi tokios įtakos. Tai daugiau ne lyderis, ne tas, kuris galėtų kažką stumti, tai yra grynai formalus etatas su formalioms užduotims. Kibernetinio saugumo srity tas lyderis yra numatytas. Aš kalbu apie kibernetinio saugumo reikalavimus, jis pavadintas – kibernetinio saugumo vadovu. O po ta sąvoka slepiasi kompetentingas asmuo arba padalinys, kurio funkcija yra užtikrinti organizacijoje kibernetinį saugumą. Tai yra gerokai daugiau negu kad saugos įgaliotinis ar galėtų (turėtų) įgaliojimų (galimybių, gebėjimų), ar netgi jis realiai yra. Tai vat toks asmuo yra numatytas ir visi senai jį turėjo paskirti. Tai būtų lyderis ir tikėtina, kad aukšto lygio vadovas, vienas iš tų – sprendimus priimančių žmonių." (E4, asmeninis interviu, 2017 m. liepos 24 d.). Paklaustas ar tradiciškai tai galėtų būti padengiama steigiant Vakarų Europos valstybėse ir JAV įprasta Vyriausiojo informacinio saugumo pareigūno (angl. *Chief Security Officer*) rolę, E4 ekspertas tokiam siūlymui pritarė: „Kažkas panašaus, daugiau gal į kibernetinį saugumą, bet kadangi pas mus viskas

bandoma padengti – vat ir už visą saugumą galėtų būti atsakingas.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.). E7 ekspertas paklaustas ar, jo manymu, būna situacijų, kai IT bendrame organizacijos veiklos procesų kontekste vis dar pozicionuojamas ne kaip integruotas sistemos elementas, o kaip šalutinis priedėlis, pažymėjo, kad tokių situacijų pasitaiko mažesnėse įstaigose, kur ir IT finansavimas vis dar būna nepakankamas: „Būna ir taip, ne visur, aš negaliu sakyti, kad ten ministerijose, bet smulkesnėse visokiose organizacijose valstybinėse tikrai nebūna, kaip teko susidurti pabendrauti, labai didelių investicijų niekas nedaro į IT ūkį.“ (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). E1 eskpertas akcentavo nepakankamas procesų ir IT teikiamų galimybių sąsajas, saugos procesų atribojimą nuo kitų veiklos sričių bei nepakankamai išnaudojamą IT teikiamą potencialą: „Aš matau, kad pas mus bendrai tas IT yra visiškai, bent jau valstybiniame sektoriuje, nesusiejamas su procesais. Procesai lieka sau, IT lieka sau, saugos dalykas išvis pakimba ore, nes pagal dokumentus jis turi būti, o sąveikos tarp jų nėra. Žmogus kaip dirbo 8 valandas, taip ir dirba, nors su IT jis galėtų dirbti 4, bet IT dirba popierinį darbą, o sauga sėdi iš šalies ir žiūri, kas čia bus.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Iš taisytinų vietų E5 ekspertas taip pat išskyrė CERT'o pobūdžio tarnybų būtinybę kiekvienoje institucijoje. E5 eksperto manymu, yra ypač svarbu, kad institucijose būtų ne tik IT ar politines veiklas vykdantys padaliniai, bet ir struktūrinis vienetas, vykdantis reagavimo į kibernetinius incidentus funkciją: „Ko trūksta organizacine prasme – CERT'o pobūdžio tarnybos ir atsakomybių valstybės institucijose. Kiekvienoje institucijoje turiu omeny. Įskaitant mūsų. Man atrodo, kad tikrai prisidėtų prie kibernetinio atsparumo didinimo komanda vykdanti CERT'o funkcijas, t.y. reagavimo į kibernetinius incidentus. Dabar pas mus yra politikos formavimo atsakingi pareigūnai, mano skyrius atsakingas už tai. Yra ITT pagalba, tačiau nėra atskiros komandos arba aiškiai apibrėžtų rolių reagavimo į incidentus. Ir tuomet reagavimo laikai nukenčia. Galbūt kompetencijos. Tai organizacine prasme siekiamybė būtų, kad vis tik organizacijoje būtų ir reagavimo į incidentus padalinys arba atskiri žmonės.“ (E5, asmeninis interviu, 2017 m. liepos 24 d.). Paklaustas apie CERT'o funkciją atliekančius centrus ir, ar būtų tikslinga juos turėti kiekvienai institucijai, E3 ekspertas pažymėjo, kad CERT'o formavimas turi prasmės tik tuomet, kai jo veikimas vykdomas CERT'o steigėjoje organizacijoje valdomoje infrastruktūroje: „Kad atliktų CERT'o funkciją, reikėtų turėti savo nuosavą infrastruktūrą, jeigu tu jos neturi, tu butaforinis, popierinis CERT'as, kuris gali pakoordinuoti. Jei jau krentam [*naudojama atsparumo modelio analogija – aut.*], tada jau nėra laiko, viskas. Su stebėsenos centrais yra dvi tokios pagrindinės praktikos, kurios tarp kitko labai gražiai sugyvena, t.y. organizacija arba aljansas turi savo techninius centrus, mes juos vadiname *operational*, nebūtinai tai SOC, tai tiesiog operacijų centrai, kurie be kibernetinio saugumo, gali dar daryti ir kitą, tinklo valdymo [*funkciją – aut.*]. Ir antras toks, pavyzdžiui, kur turi skandinavai: švedai, norvegai, privačius arba pusiau privačius centrus, kurie pasako, kas pas tave dedasi perimetre. Jie surenka iš IDS'inių sensorių visą informaciją ir tau praneša, atsakingiems žmonėms, kad va – pas jus kažkas bando lysti. Ta praktika Skandinavijoje pasitvirtino ir žmonės labai laimingi.“ (E3, asmeninis interviu, 2017 m. liepos 21 d.). Kalbėdamas apie kibernetinio saugumo sistemos roles ir atsakomybes, E1 ekspertas taip pat išskyrė organizacinio vieneto būtinybę. Pagal E1 ekspertą, toks vienetas turėtų veikti visoje organizacijoje „nepririšant“ organizaciniais saitais jo veiklų

prie konkrečių sistemų, taip pat būtina, kad šią funkciją atliekantis asmuo būtų ne tik valdymo, bet ir saugumo ekspertas: „Pagal Kibernetinio saugumo įstatymą atsiranda saugumo vadovas, jis irgi pririštas prie sistemos, tačiau daug didesnę naudą duotų ne pririšimas prie sistemos, tokios kaip vienos, bet bendrai institucijai, kad būtų kažkoks vienas, suprantantis saugą, kuris koordinuotų. Nes kai yra prie sistemų vienos, dviejų, na vienas vadovas gali būti kelioms sistemoms. Bet jei jis bus [*priskirtas – aut.*] žiūrėt toms vienai ar kelioms sistemoms, tai jis ir turės pakankamai siaurą mąstymą kaip padaryti, kad jo sistema atitiktų tuos reikalavimus, o plačiau, kad apimtų gilesnę analizę, gilesnį bendrai suvokimą darbuotojų, institucijos visos kėlimą [*žinių lygio – aut.*] darbuotojų, to vat gali ir neapimti. Tai vat, sakymas, kad institucijoje turi atsirasti per pokyčius kažkoks koordinuojantis asmuo, padalinys, kur būtų saugos vadovai priskirti sistemoms, o padalinio vadovas kaip koordinatorius žiūrėtų plačiau, tai būtų teisinga, bet tas vadovas neturi būti tik vadovas, bet ir specialistas.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). E4 ekspertas pastebėjo, kad egzistuoja pakankamai nemaža procesų, administruojančiojo personalo kaita bei vyksta terminijos dinamika, tačiau visa ši kaita neturėjo apčiuopiamo poveikio kibernetinio saugumo sistemai Lietuvoje, kas greičiausiai parodo, jog pasigendama radikaliai naujų požiūrių, leidžiančių atsakyti į kylančius klausimus ir egzistuojančius iššūkius: „Specialistų, tų, kurie dirba, administratorių saugos žmonių, tie pokyčiai nėra tiek reikšmingi. Tai, kas dabar vadinama kibernetiniu saugumu, tai buvo žinoma anksčiau ir tos visos grėsmės buvo, atsiranda tokios specifinės naujos, bet tai tiesiog situacija nuolat keičiasi. Ji keitėsi anksčiau, keičiasi ir dabar. Kažko radikaliai naujo neatsirado. Žmonės, kurie su tuo dirba, senai jie dirba savo įprastinį darbą, klausimas daugiau – galbūt reikėtų iš esmės naujo požiūrio į šitą veiklą. Gal, pavyzdžiui, daugiau žymiai dėmesio reikia skirti techninėms priemonėms? Ir gal reikėtų įvertinti iš naujo tas rizikas? Ir atsakymai tuomet atsirastų!“ (E4, asmeninis interviu, 2017 m. liepos 24 d.). E1 ekspertas atkreipė dėmesį, kad valstybinės institucijos valdo didelius kiekius piliečių asmeninės informacijos, didesnieji registrai susieti su mažesniaisiais ir egzistuoja, kad mažesniuose dėl jų mažesnės svarbos laikoma informacija nėra taip gerai apsaugota, o dėl egzistuojančių sąsajų kyla grėsmė, kad potencialiems įsilaužėliams bus prieinami ir didžiuosiuose registruose saugomi duomenys: „Yra gyventojų registras, kuriame yra tik gyventojų duomenys, bet kitos sistemos savyje šalia gyventojų registro duomenų, iš kurių vardą pavardę, AK, laiko dar papildomus [*duomenis – aut.*], kurie reikalingi jiems. Taip šalia gyventojų registro atsiranda maži registriukai, kuriuose laiko tam tikrą kritinę informaciją. Ar neturėtų būti ta informacija laikoma vieningoje vietoje, nes gal tų pačių duomenų institucijoje A, reik ir kitoms institucijoms, bet jos individualiai taip pat susirinkinėja tą informaciją, kurią galėtų naudoti savo veikloje? Jei apie mane tą pačia informaciją laiko 40 institucijų, o iš jų tik kelios rūpinasi saugumu, tai aš sunerimęs. O žmogui sužinoti, kur kokius duomenis laiko, kokios institucijos, tai yra praktiškai neįmanoma.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Kalbėdamas apie saugumo sprendimų finansavimą, E1 ekspertas pastebėjo, kad lėšos nors ir skiriamos, ne visuomet išnaudojamos pakankamai efektyviai, nevertinant realaus egzistuojančio įstaigos poreikio. Kaip pažymi ekspertas, šios problemos aktualios visiems viešojo sektoriaus IT plėtojimo finansavimo priemonėms. Taip pat akcentuotinas neišnaudojamas IT potencialas: „Visi finansavimo dokumentai, programos Europos, visi pinigai, jie daromi per kitą

galą, visiškai nevertinamas normaliai poreikis, veiklai įmonės (institucijos). Kažkas vienas galbūt susigalvojo, kad taip reikia, o pati institucija nėra tam pasiruošusi, turi būti kalbama bendrai, institucijų bendras sutarimas randamas, kad taip reikia eiti, vis dėl to tu gauni ES pinigus, pasidarai kažkokią sistemą, procesus patobulini, bet žmonės nedirba pagal juos, nes jie yra įpratę dirbti pagal seną, kad nueiti pas kolegę, nunešti dokumentus, aš dar su ja pakalbėsiu, ir bus daug įdomiau nei per sistemą perduoti el. būdu." (E1, asmeninis interviu, 2017 m. liepos 11 d.). E1 ekspertas plėtodamas diskusiją apie finansinius aspektus taip pat pažymėjo, kad turi būti laikomasi finansų skirstymo balanso, tai turėtų būti daroma formuojant adekvačias saugumo priemones ir diegiant tose srityse, kur jos labiausiai reikalingos bei neskiriant jų, kur jos nėra būtinos. Tokie balansavimo mechanizmai didina piliečių pasitikėjimą valdžia: „Tada tu, jeigu neišleidi pinigų kažkur perteklinai, tu gali išleisti pinigus ten, kur tau tikrai jų reik – dėl to atsiranda ekonominis pagrindimas. Jei kalbant apie VT institucijas, tu gali pasakyti, kad mes piliečių pinigus taupome, saugom piliečių duomenis čia ir čia, o čia nesaugome, nes mums tai neaktualu ir iš to didėja piliečių pasitikėjimas valdžia." (E1, asmeninis interviu, 2017 m. liepos 11 d.). Paklaustas apie galimas piliečių ir viešojo sektoriaus bendradarbiavimo formas, stiprinant kibernetinį saugumą, E2 ekspertas tokiems siūlymams ypač pritarė, o pateikus pavyzdžius JAV iniciatyvas *Hacking for security, Hacking for deffence* ar situacijas, kai entuziastai kuria sprendimus kariuomenei arba valstybiniam sektoriui, testuoja jų saugumą, pažymėjo, kad jau dabar vykdomos bandant sukurti kibernetinių savanorių pajėgas: „Taip, tokias iniciatyvas reikėtų stiprinti ir jau dabar apie tai yra šnekama. KAM NKSC įkurtas ir jis dabar tuo ir užsiima, net yra kuriamos kibernetinių savanorių pajėgos. Pavyzdžiui, savanoriais gali nueiti į kariuomenę, tai dabar jie daro atskirus būrius, kurie kibernetinio saugumo srityje galėtų padėti valstybei apsiginti, būti rezerve, būti pašaukti." (E2, asmeninis interviu, 2017 m. liepos 14 d.). Kalbėdamas apie veiklos tęstinumo valdymo būklę Lietuvos viešojo sektoriaus institucijose, E1 pateikė idėją, kad egzistuoja nemažai sisteminių problemų su šios veiklos organizavimu, apimančių tokius klausimus kaip egzistuojančių veiklos planų praktinių išbandymų, sisteminio požiūrio į sąsajas turinčių sistemų saugos valdymą bei tarp institucinių informacijos mainų: „Nelabai jo yra [*veiklos tęstinumo – aut.*]. Realiai yra dokumentas kaip ir parengtas. Bet jie pasirengę kaip ir turėtų, bet ar jie jį išbando, ar jis veikia. Net yra žmonių grupės, tie žmonės tikrai įtraukti į tą veiklos tęstinumą. Bet ar galima realiai skambinti institucijos vadovui 4 valandą ryte ir sakyti, kad va – pas mus sistemos veikla sutriko. Ar darbuotojas nebus nubaustas. Veiklos tęstinumo planai yra parengiami kiekvienai sistemai, bet gal reikėtų visumos. Nes, tarkim, jei „nulėkė" gyvūnų registras, gal jis nėra svarbus, bet gal dėl to negali veikti kažkokios veterinarinės sistemos registras. Bendrai tą mastą pasižiūrėti, *sumapinti* sistemas su sistemomis. Kad institucijos keistųsi info apie tai, kas neveikia ir kad jaustų pareigą ir atsakomybę prieš kitas institucijas, jei dar duomenys yra teikiami mokamai, per tas visas puses." (E1, asmeninis interviu, 2017 m. liepos 11 d.). Kalbant apie kibernetinio atsparumo tendencijas, galima būtų pažymėti, kad ekspertai sutinka, jog absoliutus kibernetinis atsparumas, kaip ir kibernetinis saugumas, yra neįgyvendinama sistemos būsena, kokiame kontekste ir valdymo lygmenyje tai būtų bandoma pasiekti: „Atsparios organizacijos nėra ir, ko gero, nebus. Ten, kur naudojama bet kokia įranga visur yra spragos. Įranga gali būti tiek ofisinė, tiek SCAD'inė (angl.

– *supervisory control and data acquisition)*“ (E5, asmeninis interviu, 2017 m. liepos 24 d.). „Bet niekada nebus taip, kad kiek tu priemonių beįdiegtum, vis tiek nebus garantijos, kad tu 100 proc. apsisaugosi. Kaip sakoma: ‘saugios sistemos nėra, yra tokia, į kurią dar neįsilaužta.’ Tai, jei pas tave neįsilaužta, nepastebi, tai dar nereiškia, kad nėra ten priešo viduj.“ (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Vertėtų pažymėti, kad toks ekspertų požiūris, ko gero, grindžiamas tuo, kad pati interneto infrastruktūra jos gyvavimo pradžioje projektuota neskiriant tinkamo dėmesio į saugumo dedamąją. Tai pripažįsta ir patys jo kūrėjai[30]. Dažnai ir programinė įranga yra kuriama taip, kad kuo greičiau ją būtų galima komercializuoti parduodant klientams. Dėl tokios skubos neretai paliekamos saugumo spragos, kurių skaičių padidina dar ir ją kuriančių programuotojų nuolatos daromos tos pačios klaidos[31]. Pasak kai kurių apklaustų ekspertų, tų spragų skaičius ateityje tik didės: „Įrangos gamintojų pasaulyje yra tiek, kiek yra, spragų yra tiek, kiek yra ir jų bus daugiau.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.), o dėl augančio bendro programinės įrangos naudojimo skaičiaus, šioje srityje galima būtų tikėtis tik saugumo padėties blogėjimo. E1 eksperto nuomone, dėl saugumo priemonių nuolatinės sąveikos su įvairių formų grėsmėmis vyksta pastovus organizacinių sistemų tobulėjimas: „Yra virusas *Wannacry* – jis šiai dienai nieko nenustebins, jis turi būti modifikuotas taip, kad veiktų kitu principu, kažką kitaip darytų, nes jei jau identifikavo virusą, žmonės ir sistemos pamatė, kad yra virusas, tai visos sistemos automatiškai atsinaujina ir jis taip jau nebeveikia ir iš tos pusės taip ir yra, evoliucija – sukuriamas virusas, tada pamatomas, sistemos prisitaiko ir jis jau nebeveikia [...] evoliucionavimas vyksta natūraliai, bet ar IT sistema [*kaip atskiras objektas – aut.*] gebėtų evoliucionuoti? Vargu, nebent ji pati savyje turėtų turėti saugos tam tikrus elementus, kažkokias ugniasienes su atsinaujinančiais aprašais, *intrusion detection system*, kažkokius saugos elementus, per kurią jis atsinaujintų.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Taip pat E1 eksperto nuomone, nepaisant nuolatinės dinamikos ir pozityvios saugos sistemų kaitos, grėsmės dėl netikėtumo faktoriaus visuomet bus vienu žingsniu priekyje: „Tu nesugalvosi visų galimų variantų, kaip užpuolikas mąstys, nes vienas užpuolikas mąsto kaip programuotojas ir bando per programinį kodą laužtis, kitas – per duomenų bazių laukus, trečias – jėga per tinklą, jei jie susijungia du į vieną vietą ar trys, tada išvis neaišku kas ten bus. Dėl to yra labai sunku sugalvoti įvairius variantus, dėl to incidentai visuomet ir yra priekyje.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.).

Šį poskyrį vertėtų užbaigti kritiniais E3 pastebėjimais apie dabartinę kibernetinio saugumo plėtojimo būklę ir kokiomis sąlygomis ši plėtotė yra vykdoma, nepaisant to, kad situacija gerėja, procesai ne visuomet vyksta taip greitai, kad atsakytų į dinamiškus saugumo iššūkius. Pažymėtina, kad analizuojant eksperto išsakytas tezes, apie sprendimų priėmimą ir jų įgyvendinimą, akcentuotina ir asmeninio atsparumo būtinybė: „Visi daug labai rėkauja, kad reik stiprinti, reikia kelti, bet jokių reliai veiksmų niekas nedaro. Ačiū Dievui bent, kad apie tai pradėjo kalbėti. Bent kažkoks progresas, bet mes niekur nestovim, mums sprendimus reik priiminėti kiekvieną minutę ir kad priimti sprendimą prasideda maivymasis, tas nenori priimti, to nėra ir hierarchija taip susidėlioja, kad realiai, paskui, neduok Dieve, kas nors

30 http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/?utm_term=.254e7d7cb902

31 https://pdfs.semanticscholar.org/5ec6/93950d1e6039e04a7b86a488e816ddcdd82e.pdf

nutinka, tai lieka atsakingas tas, kuris ištraukė laidą. Tai šitie, kurie traukia laidus turi būti labai atsparūs žmonės.“ (E3, asmeninis interviu, 2017 m. liepos 21 d.).

Poskyrio išvados – kibernetinio atsparumo suvokimas bei pozicionavimas. Kadangi nėra pakankamai aiškių nusistovėjusių sąvokų egzistuojančioje kibernetinio saugumo apibrėžimų topologijoje, prieš į ją įtraukiant naujus konceptus, tokius kaip kibernetinis atsparumas, vertėtų kiek galima aiškiau apibrėžti ir suvienodinti visą esamą terminiją. Bandymas skaidyti reiškinį konceptualiai gali įtakoti jo išskyrimą iš bendrojo konteksto ir taip sąlygoti nepakankamą jo įvertinimą, finansavimą, bendrojo palaikymo organizacijoje stoką. Kibernetinio atsparumo suvokimas turi sklisti organizacijoje jos hierarchijos vertikale iš viršaus, t.y. iš valdančiosios organizacijos grandies, žemyn. Kibernetinio atsparumo konceptai turėtų būti plėtojami augant tam tikros kibernetinės bendruomenės kibernetinio saugumo raštingumo lygiui; jie turėtų būti vienodai suprantami visų tos bendruomenės atstovų. Kibernetinis atsparumas ir saugumas turėtų būti vertinami ir plėtojami lygiagrečiai su kitais organizacijos veiklos procesais. Nustatant finansavimo prioritetus, jiems turėtų būti suteikiamas toks pats svoris kaip kitiems organizacijos veiklos procesams. Resursų paskirstymas ir veiklos prioritetų nustatymas turi tiesioginę įtaką kibernetiniam atsparumui. Skirstant lėšas saugumui plėtoti, reikėtų atsižvelgiant į konkrečios institucijos poreikius; būtinas šių lėšų balansavimas. Siekiant darnios tolimesnės kibernetinio saugumo sistemų plėtros ir jų atsparumo didinimo, būtinas procesų ir teisės aktų sugretinimas. Nepaisant pakankamai senai vykstančios viešojo sektoriaus kompiuterizacijos, IT potencialas vis dar nėra tinkamai išnaudojamas, o tai turi įtakos ir plėtojant kibernetinio saugumo procesus. Plėtojant kibernetinio saugumo priemones atsparumui didinti, būtina taikyti ne *ad hoc*, o sisteminį, diegiant valstybiniu mastu, tarp-sektorinį požiūrį. Nors kibernetinis atsparumas yra sudėtingoms adaptyvioms sistemoms būdingas konceptas, jam formuoti būtinas sisteminis požiūris, tačiau jo įgyvendinimas turėtų būti vykdomas laikantis proporcingumo, priemonių adekvatumo ir sisteminio paprastumo principų. Teigiama atsparumo didinimo kaitos dinamika pozityviai įtakoja bendruosius organizacijos procesus, prisideda prie organizacijos evoliucionavimo; saugumo formavimas turi teigiamos įtakos piliečių pasitikėjimui valdžia. Kalbant apskritai apie kibernetinio saugumo sritį, pažymėtina, jog pasigendama radikaliai naujų šios srities požiūrių, leidžiančių atsakyti į pastoviai kylančius naujus klausimus ir egzistuojančius iššūkius. Lietuvoje turėtų būti vykdomas kibernetinio saugumo įstatyminės bazės tobulinimas išgryninant konceptus ir bendros kibernetinio saugumo veiklos sričių problematiką. Tuo atveju, jei mažai reikšmingos sistemos ar registrai turi sąsajų su kitomis sistemomis ir registrais, būtina taikyti visaapimantį kibernetinio saugumo plėtojimo požiūrį, priešingu atveju, pasinaudojus mažiau reikšmingų registrų ir informacinių sistemų spragomis, gali būti sąlygojami svarbių sistemų ar registrų saugumo trūkumai.

Poskyrio išvados – žmogiškųjų faktorių įtaka kibernetinio atsparumo didinimui. Formuojant kibernetinio atsparumo priemones kritinis elementas yra žmogiškieji resursai. Valstybinio sektoriaus kompiuterizacijos pradiniuose etapuose egzistavusi kompiuterinio raštingumo problematika ilgainiui transformavosi į kibernetinio saugumo raštingumo stokos keliamus iššūkius. Dėl nuolatos vykstančios kibernetinių grėsmių dinamikos žmogiškiesiems resursams reikalingas nuolatinis kibernetinio saugumo žinių atnaujinimas, kibernetinio saugumo mokymų, žinių patikrinimo ir kitokiomis formomis;

žmogiškiesiems resursams būtinas ne tik formalus jų gebėjimų įvertinimas, bet ir jo realių gebėjimų peržiūra; svarstytina priemonė visoje valstybės tarnyboje – įvadinis kibernetinio saugumo pagrindų, kibernetinio saugumo higienos kursas, kuris būtų bendrosios viešojo sektoriaus kibernetinės kultūros formavimo pagrindu. Individualių atsakingų sprendimų priėmimui ir įgyvendinimui būtinas asmeninis darbuotojų atsparumas.

Poskyrio išvados – bendradarbiavimo kultūros formavimo ir komunikacijos veiksniai. Kibernetinio atsparumo įgyvendinimui svarbus faktorius yra tinkama ir savalaikė komunikacija, aiškus veiklų pasidalijimas, dubliavimo vengimas. Kibernetinio atsparumo didinimui kritiškai svarbus elementas yra visuotinės bendradarbiavimo kultūros diegimas, apimantis įvairius bendradarbiavimo lygmenis: tarptautinis bendradarbiavimas, tarpinstitucinis bendradarbiavimas, bendradarbiavimas tarp padalinių, bendradarbiavimas kibernetinio saugumo specialistų lygmenyje. Kibernetinio atsparumo plėtrai konkrečiame teritoriniame vienete būtinas ir to teritorinio vieneto valdžios bendradarbiavimas su visuomene. Kalbant apie institucijos ryšių palaikymą su kitų institucijų kibernetinio saugumo padaliniais bei kitais kibernetinio saugumo bendruomenės vienetais, toks ryšių palaikymas turi būti vykdomas ne IT padalinių, o specializuotų, šiose institucijose įkurtų saugos skyrių.

3.2. Kibernetinio saugumo situacijos žinojimo gerinimas siekiant padidinti kibernetinį atsparumą.

Kibernetinio saugumo situacijos žinojimą gerinantys faktoriai. Kalbėdamas apie kibernetinio saugumo situacijos žinojimo svarbą, E1 ekspertas pažymėjo, kad optimistiškai nuteikia faktas, kad tam tikri veiksmai šioje srityje jau yra vykdomi, o pats žinojimo gerinimas yra svarbus reiškinys atsparumo didinimui dėl pozityvaus jo plėtojimo metu vykstančio informacijos sklaidos poveikio, kai informacija apie pažeidžiamumus, virusus ir kitus saugumui grėsmę keliančius reiškinius plinta organizacijų tarpe ir leidžia joms proaktyviai reaguoti: „Kai buvo rengiamas kibernetinio saugumo įstatymas, buvo numatyta keli aspektai: bendradarbiavimas su privačiu sektoriumi formalizuotas, bendradarbiavimas su mokslo įstaigomis ir kibernetinio saugumo informacinis tinklas, skirtas institucijoms keistis informacija. Situacijos žinojimas – apie virusą, apie ataką – vieniems patyrūs, kitiems leidžia nuo to apsisaugoti. Kadangi tu sužinai, kaip jis veikia, ką reikia pasidaryti norint apsisaugoti ir tada kiti 90 proc. gali apsisaugoti anksčiau laiko ir taip didinti atsparumą.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). E2 ekspertas pastebėjo, kad informuotumas apie situacija yra kritiškai svarbus, nes tik informuotas žmogus yra tinkamai pasirengęs kibernetiniams pavojams: „Tai turbūt pirmas atsakymas būtų būtent tas *awareness* t.y. žmonių informuotumas apie kibernetinį saugumą, tik informuotas ir susipažinęs žmogus gali imtis tinkamų apsaugos priemonių, jei jis nežinos – ir nesiims tų priemonių. Tai vat informuotumas ir švietimas yra pirmoj gynybos eilėj.“ (E2, asmeninis interviu, 2017 m. liepos 14 d.). Kalbėdamas apie egzistuojančius informacijos mainų mechanizmus, E6 ekspertas pažymėjo, kad ES lygmeniu suformuoti pakankamai efektyvūs ir turintys aiškius informacijos sklaidos būdus ir kelius informacijos mainų tinklai. Tačiau, dėl egzistuojančio biurokratijų polinkio į silosą, visuomet išlieka tam tikra rizika, kad dalijimasis informacija, tam tikrame jos sklaidos taške, gali būti nepakankamai efektyvus: „*Pettyos* ir *Wannacry*

atveju, [...] pagal NIS'o direktyvą yra įkurtas CERT'o tinklas ir visa Europa susijungusi į jį. Yra inicijuota bendradarbiavimo procedūra – *full corporation* [*pilnas bendradarbiavimas – aut.*]. Visi susijungė į *chat*'us [*pokalbius internetu – aut.*], operacijų lygio žmonės ir jie komunikavo. Kiekvieną dieną rengdavo *site report*'us [*esamos padėties ataskaitas – aut.*] apie situaciją visoje Europoje, informacija paskui eidavo į žemesnį lygį, nacionaliniu mastu, paskui paskirstoma pagal kompetenciją, tarkim, operatoriams pateikiama tam tikra informacija, valstybinėms institucijoms, žvalgybos institucijoms atskira informacija. Tą, ką Europos visi CERT'ai tirdami ir savo duomenis turėdami sujungtą į vieną *situation reportą* ir dalinasi. Dar yra, MISP'as[32] [*kenkėjiškos programinės įrangos informacijos dalinimosi platforma –aut.*]. Ta informacija visuomet vaikšto. Mes kaip CERT'as dalinamės su operatoriais visada, o operatoriai vėliau gali leisti savo vartotojams įspėjimus. NKSC dalinasi informacija su kritinėmis infrastruktūromis, valstybinėmis institucijomis [...] – kiek tas efektyvu tas info dalinimasis, čia kitas klausimas. Iš senų laikų – kas valdo informaciją tas yra Dievas." (E6, asmeninis interviu, 2017 m. liepos 26 d.). Grėsmių dinamikos kontekste, kai reikia žaibiškai keistis informacija, jos sklaidos ribojimas vertintinas tik kaip neigiamą efektą galintis duoti reiškinys – tai tarsi mitologinis, galvą smėlyje slepiančio stručio efektas, kai organizacija užsidaro savyje ir atsiriboja nuo išorinės informacijos. Pasak E1 eksperto, tokia saviizoliacija gali tik pagreitinti organizacijos kibernetinio saugumo sistemos pažeidimą: „Jeigu įmonė sėdi užsidariusi savo ūkyje ir žiūri tik savo sistemas ir nežiūri kas darosi aplinkui, tai yra laiko klausimas, kada juos nulauš ir kaip skausmingai jiems tai bus." (E1, asmeninis interviu, 2017 m. liepos 11 d.). Todėl tam tikrame kibernetinio saugumo perimetre būtina užtikrinti svarbios informacijos tėkmę įvairiomis kryptimis tiek sistemos viduje, tiek jos išorėje, horizontaliai ir vertikaliai – tai ženkliai pagerintų situacijos žinojimą ir padidintų pasirengimo apsisaugoti nuo kibernetinių incidentų potencialą: „Ką mes bandome padaryti – tai, kad jie ta informacija kuo efektyviau dalintųsi. Nes jei informacijos nesidalinsi, kas iš to, kad tu žinai? *Petyos* ir *Wannacry* atvejis parodė, kad daug kas naudoja ir senas operacines sistemas, patikrinome LT sistemas, buvo 150 pažeidžiamų sistemų. Tas 150 buvo galimos aukos, iš jų dar daugiau. Informavome – *Petyos* atveju jau buvo likę tik 30. Bet vat *Petyos* atveju, jei būtų informacija suvaikščiojusi iš pačios Ukrainos, gal net mažiau būtų buvę aukų." (E6, asmeninis interviu, 2017 m. liepos 26 d.). E1 eksperto manymu, būtina stebėti net geopolitinę situaciją, nes egzistuoja tendencijos, kad incidentų skaičiai išauga vykstant reikšmingiems politiniams įvykiams, todėl visų šių reiškinių stebėsena ir bendros situacijos žinojimas yra kritiškai būtinas atsparumui didinti: „Žinojimas situacijos, tos pačios geopolitinės, pratybos vyksta (NATO) – padidės atakų skaičius iš kitos pusės. Rinkimai Ukrainoje – vėl kažkas, rinkimai Olandijoje, Prancūzijoje, JAV, Didžiojoje Britanijoje – irgi padidėja kiekiai, pasiviešina vienų žmonių pašto dėžutės, kitiems kažkas neveikia. Bandoma sukelti nepasitikėjimą sistema, žmonėmis. Tad būtent tas geopolitinės situacijos stebėjimas leidžia daryti prielaidas, kad kažkas gali atsitikti, kad būti pasiruošus stebėti tam tikrus dalykus. Lygiai tas kalbant apie energetiką – yra kažkas Ukrainoje, elektra dingo. Pas mus pažiūri – gali būti / negali būti. Lygiai tas pats ir kituose [*sektoriuose – aut.*]. **Žinojimas yra labai svarbus atsparumui.**" (E1, asmeninis interviu, 2017 m. liepos 11 d.). Tačiau tarp apklaustų ekspertų taip pat buvo manančių, kad šią informaciją

32 http://www.misp-project.org/

organizacijoms būtų pakankamai sudėtinga suvaldyti: „Pakankamai sudėtinga valstybinei organizacijai – ar ji galės tą žvalgybinę informaciją suvaldyti.“ (E6, asmeninis interviu, 2017 m. liepos 26 d.). Taigi, darytina prielaida, kad kažkurioms iš esamų Lietuvos kibernetinio saugumo sistemos institucijų vertėtų skirti resursus šį procesą valdyti. Paklaustas ar reikėtų formuoti specialią sistemą, galinčią vykdyti išorinės sistemos stebėseną, nustatyti potencialius atakų vektorius bei vertinti tokius reiškinius kaip geopolitinė situacija, E4 ekspertas pažymėjo, kad tokie procesai iš dalies jau vyksta: „Geopolitinė situacija visiems žinoma, ne tik apie artimiausią kaimyną, bet ir tolimesnius. Kažkas stebi situaciją, analizuoja tuos visus naujus vėjus. Juolab, tos visos saugos priemonės, jos visos integruotos. Vyksta *online* palaikymas iš gamintojo pusės [*programinės įrangos spragų atveju – aut.*], iš savo pusės vėlgi renka informaciją iš įvairių šaltinių. Informacija mus pasiekia.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.). E5 ekspertas, pažymėjo, kad kibernetinio saugumo informacijos žinojimas yra svarbus dalykas kibernetinio atsparumo didinimui. Eksperto nuomone, tam ypač reikalingas išankstinis prognozavimas, apie kurį kalbant, eksperto nuomone, nėra žinoma, kad kokia nors organizacija turėtų dedikuota padalinį būtent kibernetinėms grėsmėms stebėti ir prognozuoti: „Reikia analitikų gebėjimų, ne tik reaguojančio personalo, bet ir prognozuotojų. Gal tai kažkiek persidengia su VSD funkcijomis. Tačiau nesu girdėjusi, kad jie turėtų dedikuotą padalinį kibernetinėms grėsmėms.“ (E5, asmeninis interviu, 2017 m. liepos 24 d.). Su E1 ekspertu diskutuojant apie eiliniam darbuotojui būtinos turėti kibernetinio saugumo informacijos apimtis, nagrinėtas klausimas, kiek gilios turėtų būti eilinių darbuotojų žinios apie organizacijos valdomą kritinę infrastruktūrą bei informaciją. Ekspertas pažymėjo, kad nereikėtų paprastų darbuotojų perkrauti sudėtinga kibernetinio saugumo informacija, tiesiog reikėtų pažymėti valdomo kritinio objekto svarbą ir apmokyti, kaip reikėtų su tokiu objektu elgtis: „Nereikia apkrauti nereikalingu informacijos kiekiu paprastų žmonių, svarbu, kad jie žinotų principus saugos, kad laikytųsi standartų reikalavimų, pradedant slaptažodžių politikomis, baigiant kompiuterių rakinimu, kuo jie tą bazę išlaikys ir „pasikels“. Bet pradžioj to tikrai nereik. IT administratoriai turi žinoti daugiau, kas yra svarbu, kad žinotų, kokia informacija pas jį yra kritinė. Dėl to darbuotojai turi žinoti klasifikavimą informacijos. Kaip, kur su kokia informacija reikia elgtis. Jeigu jie žinos bent tą, jiems nereikia žinoti, kaip, kokioje sistemoje ji yra apdorojama, tiesiog žinoti jei aš dirbu su ta informacija, aš turiu būti truputėlį atsakingesnis, nepalikti kompiuterio pas kažką kabinete, svečiuose pas rangovą be priežiūros.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Atsakydamas į klausimą, ar dirbančiųjų institucijoje tarnautojų žinojimas apie jų institucijos sistemomis teikiamų paslaugų kuriamą vertę piliečiams, galėtų prisidėti prie sistemos atsparumo didinimo, E4 ekspertas pažymėjo, kad tai yra vienas iš galimų būdų, tačiau lygiagrečiai jam reikėtų ir adekvataus įvertinimo šioms sistemoms nustatant kritiškumo lygius: „Tai vienas iš tokių būdų, vėlgi ypatingos saugos infrastruktūra, ypač svarbios paslaugos, kurių neteikimas sutrikdytų šalies veiklą, ar padarytų didelę žalą – tai ir yra esminis kriterijus, kas turėtų pakliūti į tą sąrašą. Metodika savaip tą klausimą sprendžia, nes reikia kažkaip viską formalizuoti. Tad rezultatas gali gautis ne visai toks, kurio tikėjaisi. Kažkas labai susireikšmino, kažkas – priešingai.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.).

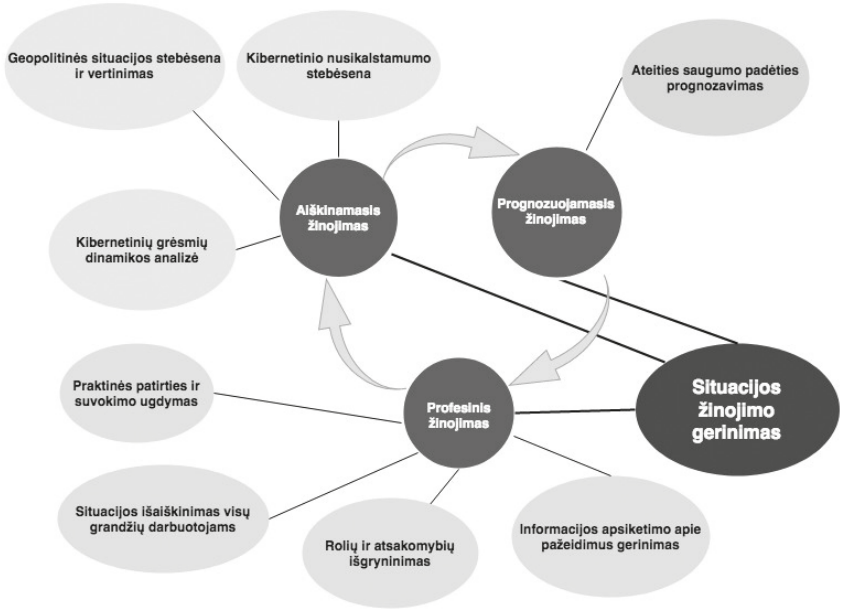
Kibernetinio saugumo situacijos žinojimo gerinimo iššūkiai. Kalbant apie dabartinę situacija kibernetinio saugumo srityje ir egzistuojantį problemos masto suvokimą, E4 ekspertas pažymėjo, kad dabartinėje situacijoje dauguma diskusijų primena viešojo pobūdžio kalbėjimą, tad sunku pasakyti, ar atsakingi už srities sprendimų priėmimą asmenys suvokia problemos mastą: „Na, vėlgi, informacijos apie tai kas skelbiama ir kas prieinama, t.y. ką kiti šneka, man panašiau į tokį viešo pobūdžio šnekėjimą. Nelabai galiu suprasti, ką gi tie žmonės realiai suvokia ir, ką jie galvoja. Tad, šiuo atveju, gali būti, kad jie puikiai suvokia situaciją, bet to neišreiškia, o gal ir priešingai." (E4, asmeninis interviu, 2017 m. liepos 24 d.). E4 ekspertas pritarė nuomonei, kad esant resursų trūkumui sudėtinga užtikrinti ir vykdyti tinkamą bei savalaikę komunikaciją. Jis taip pat išreiškė pritarimą teiginiui, kad valstybiniame sektoriuje vis dar egzistuoja informacijos riboto dalijimosi – informacinio siloso kultūra. Skeptiškas E4 ir Nacionalinio kibernetinio saugumo centro atžvilgiu pagrindinė to priežastis – neaiškūs saugumo centro veiklos pasiekimai, platinamos kibernetinio saugumo situacijos informacijos vertės stoka: „Savo veiklą pradėjo Kibernetinio saugumo centras ir jis aktyviai tą daro [*vykdo informavimo veiklas – aut.*], tik aš nesu informuotas apie jo kasdienę veiklą ir jų pasiektus rezultatus, t.y. jie skelbia metines ataskaitas, bet man asmeniškai kažkokios esminės naujos informacijos kaip specialistui, tai nelabai yra. Tai daugiau toks piarinis ėjimas. Galbūt ten yra informacijos įdomios ne specialistui. Bet visi žinome, kad kibernetinių incidentų skaičius sparčiai auga, o galo tam kol kas nesimato. Tam va žinomumui tos srities tai prideda – kai skamba kažkoks pavojaus signalas ir tai prisideda prie tos srities aktualumo. " (E4, asmeninis interviu, 2017 m. liepos 24 d.). Nagrinėjant informacinio žinojimo aspektus, pastebėtinas ir melagingų naujienų (angl. *fake news*) bei informacijos perkrovos daromas neigiamas efektas, kai dėl skirtingos valdomos informacijos, skirtingos institucijos ne visuomet gali tinkamai reaguoti, o susidarius sąmyšiui, formuojasi tinkama terpė naujiems kibernetiniams nusikaltėliams įsilieti į vykstančius procesus ir vykdyti nelegalią veiklą. Tokiame sąmišyje gelbstinčia priemone laikytina ES vykdoma informacinio situacijos ataskaitos inicatyva: „Dabar kai ta informacijos dalijimosi era, visi dalinasi, bet tikrai nežinai, ar ta informacija tikra ar ne, viena dalis šneka taip, kita – taip ir jau pasimeti paskui [...] galiausiai paaiškėja, kad tai ne *Petya*, o tai *NotPetya*. Kiti dar pasinaudoja atakom, atsiranda dar kažkas iš šono, susimaišo." (E6, asmeninis interviu, 2017 m. liepos 26 d.). Diskutuojant apie tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje kaip kibernetinio saugumo situacijos žinojimo priemonę, pasirodo, kad ji gali būti trikdoma net ir pernelyg formalus bendravimo, kurį E3 tiesiai įvardina – susireikšminimu: „Taip, ir žmogiškieji kartais pamaišo, kad yra mūsuose toks dalykas kaip susireikšminimas. Kiekviena visuomenė tą turi ir mes nuo to niekur nepabėgame. Tai vat susireikšminimą turi eliminuoti bendra komanda." (E3, asmeninis interviu, 2017 m. liepos 21 d.). Kalbėdami apie tarpinstitucinius ryšius, ekspertai pastebi, kad jie egzistuoja, tačiau jie egzistuoja asmeninių ryšių pagrindu: „Jis egzistuoja, bet deja tiktai asmeninių ryšių pagrindu. Jei tu mane pažįsti, nes kas susiję su saugumu yra ypatingai jautru, tai todėl arba tu pasitiki žmogum, arba ne. Už žmogaus stovi institucija, jei žmogus išėjo į kitą instituciją, reiškiasi tavo pasitikėjimas krypsta kitur. Jei žmogus parodė nekompetenciją, tai parodė ją prieš visus, tu to nepaslėpsi." (E3, asmeninis interviu, 2017 m. liepos 21 d.), ir migruoja iš vienos organizacijos į kitą, kartu su šiose organizacijose migruojančiais

specialistais: „Iš specialistų pusės vyksta migravimas iš vienos institucijos kompetencijų srities į kitos institucijos t.y. specialistų lygmeny jie nėra tokie labai reikšmingi. Atsiranda nauji reikalavimai, kas stipriai persidengia su esamais, t.y. nauji žmonės – nauji specialistai, su jais ateina nauji vėjai, bet jie nėra tokie radikalūs." (E4, asmeninis interviu, 2017 m. liepos 24 d.). Taigi informacijos sklaidai bei situacijos žinojimui nemažai įtakos turi ir profesinis kibernetinio saugumo sistemos darbuotojų mobilumas. Šių teiginių taikyti visoms kibernetinio saugumo sistemoms negalima, tačiau panašu, kad bent Lietuvos viešojo sektoriaus organizacijose tai reikšmingas fenomenas. Kalbėdami apie kibernetinio saugumo situacijos žinojimo gerinimą ekspertai išskyrė įvairius būdus, vienas jų dedikuoto specialisto skyrimas šiems procesams valdyti: „Nuo įmonės priklauso, turėtų būti dedikuotas žmogus, tai negali būt tik IT administratorius, nes IT administratoriaus funkcija yra tokia, kad padaryti taip, kad veiktų sistema ir, kad būtų patogu. O saugos specialisto – tai turi daugiau jis apgalvoti. Kad būtų patogu – yra mažiausias jo uždavinys. Tai turi būti sauga, *update*'ai [*atnaujinimai – aut.*], pažeidžiamumai tinkle, švietimas nuolatos." (E6, asmeninis interviu, 2017 m. liepos 26 d.). Kaip ir kiekvienoje kitoje kibernetinio atsparumo didinimo srityje, ekspertai akcentavo personalo mokymus: „Čia tiktai mokymai. Mokymais, imitacijomis. Aš žinau kelias institucijas, netgi ne kelias, pas mus yra laikas nuo laiko darbuotojams yra išsiunčiami laiškai: 'atvažiavo jūsų siuntinys, užeikite į tokį puslapį, jūs va čia galite įvesti savo vardą slaptažodį arba pasitikrinti tą siuntinį.' Paskui, kai apie tai surenkama statistika, kiek žmonių paspaudė, kiek nuėjo į puslapį, kiek atidarė laiško priedą, arba kiek informavo tuos, kurie stebi saugumą, statistika paviešinama. Pirmu atveju, buvo labai daug nuėjusių, atsisiuntusių failą ir t.t. Antru atveju, jų žymiai sumažėjo. Toks žmonių švietimas efektyviausias yra, nes išbando, pamato viską ir pradeda suvokti. Tu nebaudi iš karto žmogaus, nes reik žmogui paaiškinti, kodėl tai nėra gerai." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Pažymėtina E5 eksperto iškelta idėja gerinti kibernetinio saugumo informacijos žinojimą vykdant grėsmių analizę ir rizikų nustatymą bei prognozavimą valstybiniu mastu: „Grėsmių analizę, rizikų nustatymas valstybiniu mastu. Prognozavimas, atakų ir panašių dalykų – konkrečiai neįrašytas jokiai institucijai į funkcijas. Kibernetinio saugumo įstatyme apie grėsmes nėra kalbos, apie jų analizę juo labiau. Apie kibernetinę gynybą įstatymas irgi nekalba. Tai vat kibernetinės gynybos, grėsmių analizės funkcijos galėtų irgi būti to vieno langelio principu priskirtos NKSC, tokiu atveju, jeigu jie dedikuotų savo pajėgumus, analitikus, galėtų skleisti tą informaciją ir valstybės institucijoms." (E5, asmeninis interviu, 2017 m. liepos 24 d.). Įdomus ir E6 eksperto siūlymas rengti organizacijose kibernetinio saugumo pusryčius, kurių metu būtų aptariamos kibernetinio saugumo problemos – tokia praktika yra taikoma kai kuriose užsienio šalyse: „Yra gera koncepcija kai kuriose įmonėse kiekvieną mėnesį, pavyzdžiui, užsienyje būdavo boso pietūs arba boso pusryčiai, o dabar padaro, tarkim, švietimo valandą ir jie apkalba kokios grėsmės yra šį mėnesį, pavyzdžiui, šį mėnesį *phishing* atakos plito labai daug, ypač su bankais daug aukų. Ir va tokios apmoko vartotojus. Susirenka su žmonėm, jei tai yra didelė įmonė,susirenka departamento lygmenyje, nes departamentų direktoriai dažniausiai arba kažkokio skyriaus, jie būna atitrūkę nuo tos srities, o paskui jie ištransliuoja žinią savo viduj darbuotojams." (E6, asmeninis interviu, 2017 m. liepos 26 d.). E7 eksperto manymu, labai svarbu aiškinamasis darbas, kad darbuotojai suvoktų saugumo užtikrinimo svarbą, o ne aklai vykdytų su saugumo

formavimo priemonėmis susijusius nurodymus: „Darbuotojams reikėtų paaiškinti ne aklai: 'taisykles vat įvedžiau ir viskas, vykdyk!' Kaip, kad: 'kasam griovį nuo tvoros ir iki pietų,' o dėl ko kasam, niekam neaišku. Todėl žmones irgi reikia lavinti ir aiškinti, dėl ko atsiranda tos taisyklės, kad čia ne tam, kad uždrausti tau naudoti internetą." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Vienas iš kibernetinio saugumo situacijos žinojimo aspektų pabrėžia, kad reikia žinoti net kokie procesai vyksta pačioje įmonėje, tai reikalinga siekiant kontroliuoti ryšių ir informacijos srautus bei vykstančius procesus, nustatyti potencialius saugumo metrikų nuokrypius nuo įprastinių ribinių normų, įvairias kitas anomalijas. Kalbėdamas apie šią sritį E6 pritaria tokių veiklų vykdymui, eksperto teigimu, anomalijų stebėsena yra kritinis uždavinys, o ypač – anomalijų stebėsena yra labai svarbus bendrai organizacijos saugumo kontrolei: „Tu žinai, kad, tarkim, šitas aukštas visi srautai Europoje vyksta ir vieną naktį rytų kryptim. Tai jau kažkokia anomalija. Ne vienoje organizacijoje esu girdėjęs tokių atvejų, kai viskas atrodo tvarkingai ir 12 valandą nakties ar po 12 įvyksta keli „nusibeldimai" toj pačioj šaly į vieną miestą. Bet pastoviai, ir nieko nėra, nežino kur virusas, nieko. „Prisiduoda" [*informacijos nesiunčia – aut.*]. Kaip papinginimas [*patikrinimas ar kompiuteris pasiekiamas per Interneto protokolo pagrindu veikiantį tinklą – aut.*]. Va tokias anomalijas užfiksuoti gali, aišku reikia įrangos, žmonių, taisykles turi susiprojektuoti, jeigu ten srautas į tą šalį padidėja, tai kažkoks indikatorius – pasiaiškinti kodėl. Jei dar ne darbo metu, tai ypač. Daug kas iš įmonių, nežinau kiek tas padeda, bet jie stebi visą srautą nedarbo metu, nes niekas nedirba – niekas neturėtų vykti. Pagrinde tik į tuos produktus turėtų jungtis, jei kažkokie *update*'ai yra uždėti. Griežta kontrolė įrenginiams: nešiojami įrenginiai, *laptopai*, telefonai. Tai padidinta rizika yra." (E6, asmeninis interviu, 2017 m. liepos 26 d.). Kalbant apie bendrąjį kibernetinio saugumo situacijos žinojimą organizacijoje, pažymėtina, kad valdančioji organizacijos grandis nebūtinai turi būti susipažinusi su specifinėmis kibernetinio saugumo detalėmis, tačiau kritiškai yra svarbus bazinis kibernetinis raštingumas, kuris prasideda nuo komunikacijos apie kibernetinio saugumo svarbą. E3 eksperto teigimu, Lietuvoje kibernetinio raštingumo srityje ir jos komunikacijoje kol kas yra nepatenkinama padėtis: „Kuo žmogus yra, kaip mes vadiname, labiau prie staklių, tuo jis labiau suvokia pažeidžiamumą, atsparumą, kritiškumą, kam gali daryti [*įtaką – aut.*], kuo lipama piramide į viršų, tuo suvokimas mažėja. Nesakau, kad iš principo yra blogai, negali juk kiekvienas vadovas žinoti tam tikrų aspektų, tačiau suprasti bendrą padėtį ir svarbą – turėtų. Todėl, kad kiekvienas žmogus, nepriklausomai nuo to, ką jis užima, turi turėti elementarų kibernetinio saugumo raštingumą. Ko pas mus, deja, nėra. Kai tik tai prasideda kibernetinio saugumo, atsparumo, tai to raštingumo nėra. Tai vat tas iškomunikavimas ir parodymas svarbos prasidėtų nuo raštingumo didinimo, jeigu bus raštingas finansistas ir bus raštingas ministras didžiosios dalies problemų jie jau nebekels, nes jie supras, kad slaptažodžių negalima kabinti – viskas." (E3, asmeninis interviu, 2017 m. liepos 21 d.). Kibernetinio raštingumo, kuris turėtų būti prilygintinas, pavyzdžiui, teisiniam raštingumui, lygio kėlimas yra svarbus ir tuo, kad jam augant didžioji dalis jo padengiamų klausimų tiesiog pašalinami iš organizacijos saugumo užtikrinimo dienotvarkės uždavinių, tokiu būdu, organizacija gali susitelkti ties sudėtingesnėmis kibernetinio saugumo veiklomis. E1 ekspertas pažymėjo, kad neretai atakos metu pasitaiko, jog incidentą turinčius suvaldyti atsakingus darbuotojus apima panika, tad jo buvo paklausta kokiu

būdu pagerinti darbuotojų funkcijų žinojimą, ką jis turėtų daryti, kaip pasirengti, kad ta panika sumažėtų, ekspertas išskyrė pratybų vykdymą: „Pratybos, vienareikšmiškai, mokymai-pratybos, inscenizavimai kuo daugiau praktinio patyrimo [...] – viskas priklauso nuo to saugos vadovo, to koordinatoriaus, kuris plačiau žiūri. Jei jis pradės rengti saugos mokymus kitiems saugos specialistams, ne tik IT specialistams: sekretorei, administratorei, per tą ir pasireikš, padės ugdyti, realiai gali saugoti perimetrą visokiom priemonėm, ateis laiškas administratorei į asmeninį paštą ir viskas tuo pasibaigs, visos saugos priemonės. Nes per socialinę inžineriją, viską perims.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Lietuvoje kibernetinio saugumo infomacijos mainams yra formuojamas Kibernetinio saugumo informacinis tinklas, kurio valdytojas yra Nacionalinis kibernetinio saugumo centras. Lietuvos kibernetinio saugumo įstatyme Kibernetinio saugumo informacinis tinklas yra įvardinamas kaip „saugi informacijos mainų platforma, kurios paskirtis yra dalytis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir bendradarbiavimą tarp kibernetinio saugumo informacinio tinklo narių kibernetinio saugumo srityje“ (Lietuvos kibernetinio saugumo įstatymas, 2014). Ekspertai, paklausti apie galimus būdus suformuoti Kibernetinio saugumo sklaidos centrą, kuris visiškai kontroliuotų kibernetinio saugumo informacinį foną, išreiškė nuomones, kad būtent formuojamas tinklas ir turėtų atlikti tokią funkciją: „Galėtų dalintis gerąja praktika. Jie šią idėja lyg ir rutulioja, nes bus įsteigtas tas kibernetinio saugumo tinklas tas [*informacinis – aut.*]. Vizija dar nelabai aiški, nes nemačiau nuostatų, bet idėjos yra kaip tik šitos. Informacijos sklaidos, gerosios praktikos mainų. Apie grėsmių analizę nebuvo užsiminta.“ (E5, asmeninis interviu, 2017 m. liepos 24 d.). E4 ekspertas nuogąstavo, kad nors tinklo iniciatyva ir gera, tačiau egzistuoja rizika, jog į jį bus žiūrėta pernelyg formaliai ir nesusiformuos tokiam dariniui būtinas elementas – bendruomenė: „Kibernetinio saugumo centras ruošiasi paleist kibernetinio saugumo informacinį tinklą. Teko jį testuoti, sumanymas yra geras ir, kad tai yra informacijos apsikeitimas, kad būtų greitas ir ten jis yra apsaugotas. Klausimas kiek juo norės naudotis patys tie institucijų naudotojai. Ar žiūrės formaliai: ‘kol manes nėra, čia man neįdomu,’ ar visgi bus kažkokia bendruomenė tinklo sukurta.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.). Atskirai verėtų pažymėti, kad bent pagal tai, kaip Lietuvos Respublikos kibernetinio saugumo įstatyme apibrėžta kibernetinio saugumo informaciniame tinkle skelbiama informacija, susidaro įspudis, kad pagrindinis jo uždavinys yra vykdyti informavimo apie suinteresuotų šalių kontaktinius duomenis funkciją: „Kibernetinio saugumo informaciniame tinkle skelbiama aktuali viešojo administravimo subjektų, valdančių ir (arba) tvarkančių valstybės informacinius išteklius, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų, elektroninės informacijos priglobos paslaugų teikėjų ir ypatingos svarbos informacinės infrastruktūros valdytojų paskirtų asmenų ar padalinių, atsakingų už kibernetinio saugumo organizavimą ir kibernetinių incidentų valdymą, kontaktinė informacija.“ (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014). Su E1 ekspertu aptariant stebėsenos procesus, kaip informacijos rinkimo priemonę, eksperto buvo paklausta, kiek reikėtų tokias priemones plėtoti, nemažai privačių organizacijų turi SOC centrus, kur sėdi prie stebėsenos ekranų (angl. *dashboards*) žmonės bei vykdo stebėseną, bet gal tokia priemonė yra pernelyg pasyvi?

Kiek tokios priemonės galėtų būti patobulintos, kalbant apie visą stebėsenos procesą? Ekspertas pažymėjo, kad tai ganėtinai brangi, tačiau viena iš techninių priemonių, leidžianti padidinti organizacijos kibernetinį atsparumą: „Monitorinimas [*stebėsena – aut.*] turi būti, bet dabar kai įmonės taupo resursus, tas pats administratorius, šalia sistemos veikimo parametrų stebi ir anomalijas tinkle, serveryje, bet tokio kaip saugos išsiskyrimo nėra. Dėl to klausimas yra kitas, kiekvienai institucijai turėt per brangu būtų, kaip bebūtų, ten dviem šimtam žmonių turėti atskirą SOC'o komandą yra nenaudinga, tad kodėl paslaugos nepirkti, trečios šalys teikia tą paslaugą. Kitas dalykas, galim pakankamai pigiai pasistatyti, susidėlioti infrastruktūrą ir tu gauni *alert*'us. Tas pats pažeidžiamumų skanavimas, kuris yra skirtingai nuo monitoringo, bet jis padeda užbėgti įvykiams už akių, nes nesužiūrėsi visko savomis rankomis, dėl to naudoji pažeidžiamumų valdymo sistemas, kurios surenka info iš atskirų DB, praskanuoja infrastruktūrą, pasako, kur yra pažeidžiamos vietos, per kur tave gali laužti, šiek tiek tam gali užbėgti**. Čia daugiau nei monitoringas, bet viena iš techninių priemonių kaip pasididinti atsparumą.** Monitorinimas šiaip bendrąja prasme nelabai padidins, nes tu tiesiog tą žalą patirsi mažesnę, nes monitoringe tu nepamatysi nieko iš anksto. Va tas pažeidžiamumų valdymas yra kur tu pamatysi iš anksto. O monitoringas tu matai kai tave laužo, tai nuo tavo gebėjimo greitai reaguoti priklauso kaip tu susitvarkysi**. Tai būtent reikia sakyti, monitoringo rezultatas parodo kiek tu esi atsparus.**" (E1, asmeninis interviu, 2017 m. liepos 11 d.). Taip pat vertėtų išskirti E7 eksperto siūlomas kibernetinio saugumo situacijos žinojimo stiprinimą vadovybės lygmeny, vykstantį iš viršaus į apačią. Eksperto manymu, tokia kryptis yra daug lengvesnė nei bandymas skleisti žinias iš organizacijos hierarchijos vertikalės apačios: „Suvokimas jeigu jis prasideda nuo viršaus – tai yra žymiai paprasčiau numesti nuo viršaus akmenuką nuo kalno negu tam mažam žmogeliukui tą akmenį užridenti iki savo vadovo, jei tokia analogiją pravedus." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Pažymėtina, kad tai turėtų būti daroma proaktyviai ir nuolatos, o ne tik įvykus kibernetinio saugumo incidentams. Kalbėdamas apie kibernetinio atsparumo žinojimo valdymo aspektus E2 pažymėjo, kad ypač naudingu veiksniu siekiant padidinti kibernetinį atsparumo situacijos žinojimą yra valdomų vertybių inventorizacijos organizacijoje atlikimas, kuris padėtų žymiai efektyviau organizuoti sistemos apsaugos darbus. Eksperto manymu, viešajame sektoriuje inventorizacijai skiriamas dėmesys yra nepakankamas: „Mažai padarytas namų darbas – inventorizacija IT ūkio. Inventorizacija, suskaičiavimas, sužiūrėjimas, suadministravimas yra labai svarbus ir turbūt pirminis [*veiksnys – aut.*], užtikrinant kibernetinį saugumą, nes jei tu nežinai savo ūkio tai dažnai nutinka toks dalykas, kibernetinio saugumo srityje, kad **tu atsparus tiek, kiek atspari yra tavo silpniausia grandis.** Jei tu pastiprini savo stipriausių sistemų saugumą, bet pamiršti savo periferines, nes hakeriai ieško silpnosios grandies ir gali per aplinkui, per kitus kelius per pažeidžiamas periferines sistemas po to pasiekti ir jau pagrindines ir pakenkti, vogti informaciją, duomenų bazes. Gal net užakcentuočiau kur nepakankamai daroma, ar net ekspertai saugumo, ypač viešajam sektoriuje, nepakankamai dėmesio skiria, tai yra inventorizacija." (E2, asmeninis interviu, 2017 m. liepos 14 d.). Apibenrinti kibernetinio saugumo situacijos žinojimo gerinimo faktoriai pateikiami 15 paveiksle.



Šaltinis: *parengta autoriaus*

15 pav. *Kibernetinio saugumo situacijos žinojimo gerinimas – ontologinė schema*

Kaip matoma 15 paveiksle, didžiausią dalį kibernetinio saugumo situacijos gerinimo veiksnių apima profesinis žinojimas. Galima daryti prielaidą, kad šiuo metu būtent šis elementas yra vienas aktualiausių viešojo sektoriaus organizacijose. Siekiant gilesnės analizės vertėtų atlikti papildomus tyrimus, apklausiant pačius darbuotojus ir bandant nustatyti kaip, jų manymu, atliekamų funkcijų žinojimas įtakoja atsparumą organizacijose bei kaip šis žinojimas galėtų būti gerinamas. Taip pat nemažai informacijos žinojimo gerinimo veiksnių apima ir aiškinamasis žinojimas. Darbo autorius pritaria apklaustų ekspertų nuomonei, kad geriausiai, šiuo aspektu, situaciją pagerinti galėtų centralizuotas valdymo sprendimas, kuris atliktų informacijos rinkimo funkcija, ją analizuotų, pagal tai prognozuotų galimus ateities sutrikdymus ir skleistų šią informaciją organizacijoms pagal kompetenciją. Žaliomis rodyklėmis paveiksle atvaizduojamas žinojimo dinamika, kuri vyksta iš ir į kiekvieno situacijos žinojimo komponentą.

3.3. Esminių pažeidžiamumų valdymo gerinimas siekiant padidinti kibernetinį atsparumą

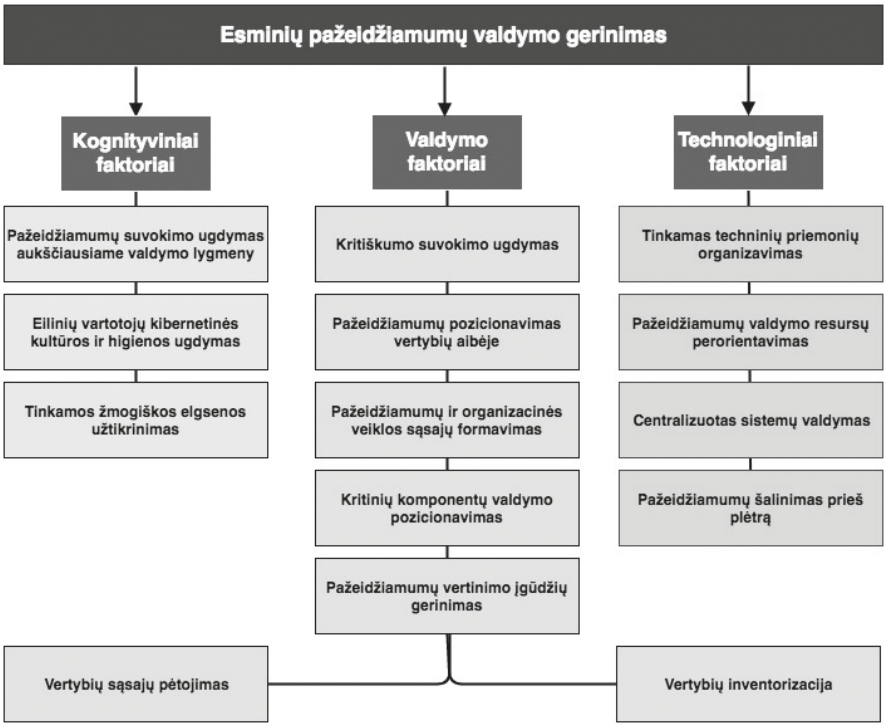
Esminių pažeidžiamumų valdymo gerinimo pagrindiniai faktoriai ir trukdžiai. Kodėl reikėtų skirti pakankamai dėmesio ir organizacijos resursų esminių pažeidžiamumų valdymui – gerai iliustruoja E1 eksperto įžvalgos. Ekspertas vertina esminių pažeidžiamumų valdymą viso atsparumo potencialo ir incidentų aptikimo kontekste, akcentuodamas,

kad didindama gebėjimus valdyti esminius pažeidžiamumus, organizacija įgauna būtiną pasirengimą, kuris iš esmės yra mobilus ir lengviau perkeliamas į kasdienines incidentų valdymo operacijas: „Žinotum pirmiausiai vietas, kurios yra kritinės ir kurias turi būti labiausiai pasiruošęs saugoti. O kai būni pasiruošęs kritinėms dalims, tas ne kritines yra padengti žymiai paprasčiau, nes tu investavai į darbuotojus, į žinių augimą, tam tikrų gebėjimų didinimą **kas sudaro galimybę būti atsparesniam**. Nereikia detaliai strateginiuose dokumentuose aprašinėti, bet jei atsiranda sąsajos IT ir verslo, bei pinigų, tada atsiranda normalus pagrindimas poreikiams." (E1, asmeninis interviu, 2017 m. liepos 11 d.). Kalbėdamas apie esminių pažeidžiamumų valdymą iš techninės perspektyvos, E2 ekspertas pažymėjo, kad pirmąja gynybos linija turėtų būti ryšio tinklai. Tai yra bazinis komponentas, tad, pagal ekspertą, pradėdama įgyvendinti kibernetinę higieną savo ryšių infrastruktūros dalyje, organizacija formuoja pagrindus ne tik esminių pažeidžiamumų valdymui, bet ir bendrojo atsparumo gerinimui: „Visa gynyba konstruojama visų pirma į tuos žinomus [*incidentus – aut.*] ko visi bijo tiek organizacijos, tiek valstybėje – atakų, incidentų, nuo kurių yra nukenčiama. Tai tie incidentai, tos atakos bet kuriuo atveju visų pirma praeina per ryšių tinklus, per „trafiką" (*ryšių srautą – aut.*] ir tik tada pasiekia organizacijas. **Todėl atsparumo valdymas ryšių tinklų sektoriuje tampa kritinis ir esminis, nes geras atsparumo valdymas, kibernetinio saugumo valdymas užtikrinamas tinklų lygmenyje**, automatiškai mažiau incidentų ir mažiau neigiamo poveikio pasiekia organizacijas. Tai vat atsparumas tinklo lygmenyje yra tas esminis valstybės požiūriu bent mūsų organizacijoje visas akcentas dedamas į atsparumą per ryšių tinklus, ryšių infrastruktūrą." (E2, asmeninis interviu, 2017 m. liepos 14 d.). Techninės priemonės, pagal E6 ekspertą, taip pat apimtų tinkamą tinklo architektūros formavimą ir proaktyvius saugumo spragų taisymus bei automatizuotą infrastruktūros stebėseną: „Aišku viena iš kontrapriemonių – visą laiką reikia užsilopyti prieš įvykstant atakoms. Yra tam technologiniai sprendimai, yra ir nemokami, kur tau patikrina visą tinklą ir kai išeina kažkoks atnaujinimas nereikia žmogui stebėti tų visų *common vulnerabilities and exposures* [*bendrieji pažeidžiamumai ir nesaugumai – aut.*], tu identifikuoji, kad pas tave yra toks produktas tinkle. Vienas iš punktų tas stebėjimas ir valdymas pažeidžiamumų yra labai svarbu, bet dar yra kitas – teisinga architektūra tinklo. Tai jei tinklas *firewall*'as pas tave viską praleidžia. Niekas to pažeidžiamumo ir neieškos." (E6, asmeninis interviu, 2017 m. liepos 26 d.). Kalbant apie valdymo aspektus, E3 ekspertas pažymėjo būtinybę užtikrinti techninių, organizacinių ir žmogiškųjų priemonių balansą ir saugos kritinių elementų ir kritiškumo laipsnio tinkamą suvokimą: „Apskritai saugumas yra visuma organizacinių, žmogiškųjų ir technologinių priemonių. Jeigu mes turime mažesnę organizacinę dalį, t.y. mažiau procedūrų, tada mes šitą dalyką pastiprint galim žmogiškaisiais resursais, kompensuoti kažkiek. Nesakau, kad visiškai. Jei nėra žmonių tai gal procedūrą sukurti. Čia toks balansavimas tarp: reiškia ta kritinė infrastruktūra – kam ji yra kritinė? Padaliniui, įmonei, valstybei, aljansui, tarkime NATO. Tu turi irgi suvokti ir susispecializuoti kam tu esi kritiškas." (E3, asmeninis interviu, 2017 m. liepos 21 d.). E5 ekspertas akcentavo IT sistemų, jų vartotojų, kompiuterinių darbo vietų ir naudotojų centralizuoto valdymo naudą esminių pažeidžiamų valdymui: „Gerintų pažeidžiamumų valdymą apskritai centralizuotas IT valdymas. VRM turi ir valdo kelias info sistemas, kurios įtrauktos į kritinės infrastruktūros sąrašą, tai bent jau jų atžvilgiu, o dar geriau visų

registrų ir sistemų atžvilgiu būtų taikomas centralizuotas valdymas. Tai reiškia ir naudotojų centralizuotas valdymas, darbo vietų centralizuoti sprendimai, atnaujinimų diegimas tiek serverinėse, tiek darbo stotyse centralizuotas. Antivirusinių ir pažeidžiamumų skanavimo centralizuoti sprendimai. Pažeidžiamumų vertinimus atliekame kasmet. Galime net numatyti, kad analogiški pažeidžiamumai gali būti, pavyzdžiui, ne VRM, o PD valdomose sistemos VSAT sistemose. Tačiau juos šalinti galime tik VRM. Kad ir tarkim antivirusinis sprenidmas PD turi atskirą,VSATas turi atskirą, policija atskirą. Atnaujinimai ten sutampa, nesutampa. Žodžiu aš čia būčiau už IT tokį stiprų centrą, kuris valdytų visą tai." (E5, asmeninis interviu, 2017 m. liepos 24 d.). E1 eskpertas pažymėjo būtinybę aiškiai nubrėžti kritinių sistemos komponentų vertybines sąsajas su organizacijos veiklos procesais ir taip aiškiai apibrėžti organizacijos IT dalies kuriamą pridėtinę vertę organizacijai. Eksperto manymu, visa tai turėtų būti įtvirtinama strateginių organizacijos veiklos dokumentų lygmenyje. Pažymėtina, kad su esminiais pažeidžiamumais susijusi veikla turėtų būti vykdoma ne tik atsitikus krizinėms situacijoms, bet nuolatos, todėl tarp prevencinių siūlytinų priemonių reikėtų įvardinti auditus: „Jeigu mes sudedame veiklos procesus, informaciją, pelną, arba net priešingai – žalą su IT procesais, su IT sistemomis, su informacija, kuri apdorojama DB, netgi iki tam tikrų įrenginių jei nusileidi ir parodai visa grandinę ir parodai, kad jeigu tas serveris neveiks arba bus atakuojamas, galima prarasti tiek pelno arba patirti tokią žalą, tuomet visiškai kitaip žiūrima. Jie aišku turi atsirasti strateginiuose dokumentuose. Bet būtent turi atsirasti tas surišimas, nes kol nėra surišimo, tol ne IT žmonės, o pvz., verslas negalės suprasti, kad tas serveris yra mums labai brangus, nors realiai jis yra 100 metų neatnaujintas, nes jam nebuvo skirta pinigų. Taip ir yra, kol kažkas neatsitinka, visi galvoja, kad viskas taip ir turi būti, o kai atsitinka būna per vėlu. Todėl didžiosios kompanijos ir investuoja į rizikų vertinimus ir auditus, kad suvesti finansinius aspektus su techniniais." (E1, asmeninis interviu, 2017 m. liepos 11 d.). E7 eskpertas taip pat pastebėjo, kad valdančiosios grandies supratimas apie kritinį IT vaidmenį organizacijai yra būtinas. Eksperto teigimu šis suvokimas turi prasidėti būtent nuo organizacijos vadovo, kuris turi suvokti, kad IT nėra tik organizacijos priedėlis, tačiau, pastaruoju metu, vis dažniau tai yra organizacijos duomenų ir ryšių su klientais valdymo pagrindą formuojantis visos organizacinės sistemos komponentas: „Eilinį kartą sakau – viskas turi prasidėti nuo vadovo. Tada kai vadovas ima suvokti, kad jeigu pas jį kažkas nutiks ir nustos veikti tų pačių klientų valdymo informacinė sistema, arba dar kažkokia kita. Jei ten užšifruos duomenis, kad jis – negalės dirbti. Jeigu jis tai pradeda suvokti ir suprasti, jis tada ima automatiškai didinti ir tų sistemų atsparumą. Bet jeigu vadovas nesupranta, tuomet nieko nebus. Nes kaip ir visur, jeigu ateina vadovas ir jam IT specialistai sako, kad: ‚mums antivirusinė baiginėjasi. Tai, o kam jums mokama, paimkit vos ne Avastą kokį ir įsidiekit, ir jums čia šito užteks' tai jeigu toks požiūris yra, tai turbūt įmonė nusipelnė, kad į ją kažkas įsilaužtų ir užšifruotų duomenis, turbūt tada taip reikia. Toks požiūris...Yra svarbesnių projektų nei informacinės technologijos, jų kaip ir nelabai matosi darbui." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Tinkamas pažeidžiamumų problemos suvokimas valdymo grandyse labai gerai iliustruotas E5 eksperto pateiktais praktiniais pavyzdžiais, apibūdinančiais situacijas, kai informacija apie egzistuojančius pažeidžiamumus sąrašų pavidalu nuolatos pateikiami institucijos vadovybei, tačiau dėl tam tikrų įgūdžių stokos deja dažnai nėra kam jos tinkamai

įvertinti, o tai sukelia ne tik finansavimo problemas, bet ir sudaro sąlygas manipuliacijai ir finansavimo gavimui tose srityse, kur jo apskritai nereikia: „Sudarius pažeidžiamumų sąrašus, trūkumų ir pažeidžiamiausių vietų informacija pateikiama mūsų departamento vadovybei ir ministerijai. Va šitam valdytojo lygmeny, deja nėra kam jų vertinti. Priimti sprendimą pagal mūsų siūlymus. Tai kartais finansavimą sunku gauti net ir kritiniam pažeidžiamumui šalinti. IT sektorius valdytojo lygmeniu, ministerijos lygmeniu irgi turėtų turėti kompetentingus žmones, pas mus čia deja, sudėtinga. O tai kelia dvejopas problemas: 1. Galima nesulaukti pritarimo, kad būtina šalinti pažeidžiamumus; 2. Atvirkštinė manipuliacija, t.y. pagrįsti investicijas, ten kur jų visai nereikėtų. IT padalinys ir valdytojas sistemos, ministerija dažniausiai, kad surastų bendrą kalbą ir vienodai matytų, kad pirma šalinimas silpnų vietų, paskui – plėtra. Dabar dažnai visų pirma plėtra, o saugos spragų tvarkymas – antraeilis dalykas. Norėtųsi, kad bent lygiagrečiai su plėtra [*saugos plėtojimas vyktų – aut.*], bet ne – iš paskos.“ (E5, asmeninis interviu, 2017 m. liepos 24 d.). E3 ekspertas papildydamas esminių pažeidžiamumų suvokimo svarbą, kaip pavyzdį pasitelkė oro navigacijos sistemas, pažymėjo, kad pažeidžiamumo suvokimas turi būti formuojamas aukščiausiu tam tikros sistemos lygmeniu, todėl būtina turėti aiškų pažeidžiamumo objektų pozicionavimą visoje būtinų apsaugoti elementų sistemoje: „Visų pirma, suvokimas, jeigu tu suvoki kaip oro paslaugų sistemos yra kritiškos valstybei, galbūt ir NATO tu esi kažkiek svarbus, nes mes palaikome ir NATO operacijas. Bet Klaipėdos laivynui mes gal nereikšmingi, bet paėmus valstybei mes galbūt esame reikšmingi. Tai tas dalykas, aišku kai tu jau išsiaiškini pas save viduje, tuomet turi sueiti visa grupė, t.y. valstybė juk yra grupė žmonių, kuri turi išsidalinti svarbus tu ar ne. Bendras sutarimas, suvokimas.“ (E3, asmeninis interviu, 2017 m. liepos 21 d.). Atskirai vertėtų pažymėti, kad tokia perspektyva ypač gerai atspindi Kopenhagos mokyklos saugumizacijos idėjas. Kalbant apie žmogiškąjį faktorių, vertėtų atkreipti dėmesį į E6 eksperto pastebėjimus. Eksperto manymu, kad ir kiek būtų efektyvios techninės priemonės, silpnąja grandimi visuomet išlieka žmogus: „Personalo švietimas visose dalyse turi eit lygiagrečiai, gal net didžioji dalis, nes žmogus gaus laišką ir jeigu jis pats paspaus, tai čia jokios apsaugos priemonės nepadės. Žmonės tokie yra, jie turbūt smegenyse yra *clickint* [*spaudinėti – aut.*] ant visko ką gauna. Tai jei tau sako nespausk ant šitos nuorodos ir nors ir parašysi, vis tiek atsiras kas paspaudžia. Žmonės, jie negalvoja, jie pripratę, nes viskas vyksta labai greitai, *click*, *click*, *click*, 3 kartus taves paklausia ar tu nori *ransomwara* įsirašyti, taip, taip, taip. Ir tada jokios technologinės priemonės tau nepadės.“ (E6, asmeninis interviu, 2017 m. liepos 26 d.). Tad visų esminių pažeidžiamumų valdymo gerinimo priemonių gausoje būtina akcentuoti personalo mokymus, kurių pagalba būtų ugdoma bendra organizacijos, sektoriaus ar valstybės kibernetinio saugumo kultūra, bei mokoma tinkamos kibernetinės higienos palaikymo ne tik sisteminiame, bet ir eilinio vartotojo lygmenyje. E4 ekspertas išskyrė vertybių inventorizacijos būtinybę ir sąsajų tarp jų identifikavimo poreikius bei pastebėjo, kad veiksminga priemone čia galėtų būti scenarijų pagrindu vykdomas sistemos sutrikimo modeliavimas arba pratybos. Bendrai eksperto manymu, viskas turėtų būti valdoma kaip ir kritinės infrastruktūros atveju – sudarant kritinių vertybių sąrašus, tačiau tuo nereikėtų apsiriboti, būtina vykdyti jų tolimesnę analizę: „Valdytojas turi žinoti ką jis turi, t.y. inventorizuoti visus savo turimus *asset*'us [*vertybes – aut.*], tai būtina. Tiek dėl turto, tiek dėl tolimesnės analizės. Tad toliau kalbant apie

atsparumą, analizuoti ryšius tarp jų, t.y. kas nuo ko priklauso, galbūt *mappinimas* [*susiejimas – aut.*], bet tai realiai yra pasirinkimas. Ar analizuoti galimų scenarijų, galimų grėsmių pagrindu. Jei, sakykime, ten kažkoks mūsų assetas dingsta / sugenda, ką tai sukels, t.y. kas dar sustos su tuo? Tai vienas iš tokių buvo bandymas padaryti, t.y. kažkokia metodika buvo identifikuojant ypatingos svarbos infrastruktūrą. Ta metodika yra, sąrašas yra, jis yra įslaptintas. Tas vienas aparatas jau apsisuko. Tai turint dabar va tokį sąrašą, inventorizavus tokią infrastruktūrą, reikėtų detaliau ją analizuoti. [...] Galima pratybas – vat nebeturim šito daikto ir kas tada. Bet tai yra veiklos tęstinumo planavimas – jis vis dar pas mus ant stalo ir turim juo užsiimti." (E4, asmeninis interviu, 2017 m. liepos 24 d.). E6 ekspertas, kalbėdamas apie dedikuotą esminių pažeidžiamumų valdymo rolę, pastebėjo, kad čia reikėtų racionaliai įvertinti organizacijos dydį, tačiau jei organizacija gali sau tai leisti, vertėtų turėti tik pažeidžiamumų valdymo ir saugumo klausimais užsiimantį specialistą: „Priklauso nuo įmonės – jei įmonė iš penkių žmonių, tai žmogaus nededikuosi, bet jei ta įmonė yra didesnė-vidutinė įmonė, aš manau, kad tai yra sveika ir teisinga turėti dedikuotą specialistą, kuris pavestas konkrečiai tik tai funkcijai, kaip pvz., saugos įgaliotinis, bet jis negali turėt kažkokių kitų funkcijų: 'ai neturi šiandien darbo, tai nueik kompiuterius pajungt, spausdintuvą,' nes jis turi domėtis ta sritim, nes jei tu saugos sritim nesidomi, reaguoji tik į tai ką tau praneša gamintojas, o kas vyksta visoje saugos bendruomenėje, tu nežinai." (E6, asmeninis interviu, 2017 m. liepos 26 d.). E1 ekspertas atkreipė dėmesį, kad būtinas veiksnys yra saugos principų praktinis taikymas ir pats vienas tinkamai atliekamas saugos principų reglamentavimas nėra pakankamas, būtina užtikrinti dokumentuose nustatytų saugos principų praktinį įgyvendinimą: „Tam tikri principai ir dabar nustatyti. Kitas dalykas yra sureglamentavimas, nurodymas kaip ką daryti yra tvarkingas, bet kaip tas praktikoje įgyvendinama? Aš tikrai abejoju, kad ten tegu neįsižeidžia joks miestas, bet Kelmės rajono savivaldybės finansų valdymo sistema, ar ten atliekamas jos testavimas? Nes ten iš viso yra 1 arba 2 IT specialistai arba iš viso ta paslauga yra *outsourcinama*, tai klausimas kaip ten veikia? Gal ji nebus labai kritinė, bet su ja turi būti žaidžiama, testuojama sužiūrima kaip darbuotojai geba. Būtent tas praktinis aspektas... Iš teisinės pusės reglamentavimo viskas atrodo OK, bet tas praktinis panaudojimas vos net turėtum daryti įmonės auditą. Nes kai paprašysi, kad tau užpildytų, visi sakys: ‚taip, mes darom', bet praktika bus visai kitokia." (E1, asmeninis interviu, 2017 m. liepos 11 d.). Pažymėtina, kad kalbant apie esminių pažeidžiamumų apsaugą, nuo diskusijų apie kritinę infrastruktūrą, kuri valstybiniu lygmeniu yra esminių pažeidžiamumų valdymo objektas, visiškai atsiriboti nepavyko. Tačiau E7 eksperto lakoniški pastebėjimai šiuo klausimu tik patvirtino literatūroje egzistuojančias tezes apie kibernetinio saugumo tyrimų srities problematiką: „Ir kiek aš žinau, tas dalykas yra daromas [...]. Žinau daugiau nei galiu pasakyti, nes tai biški tarnybos paslaptim gali baigtis [...]. Yra tam tikros įmonės, kuriose jie tą darbą daro. Tobulumui ribų nėra, ne viską galiu pasakoti. Bet matai, visos tos kritinės – vandens, elektros, dar kažkas. Tos, kurios nustatytos vyriausybės kaip saugotinos sritys, tai ten saugumas yra didinamas. Yra stebimi tinklai ir dar kažkas." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Tad akivaizdu, kad kibernetinio saugumo sritis yra tiek jautri, kad gilesnė jos analizė, ypač apimanti tokius aspektus kaip kritinės infrastruktūros apsauga yra ypač sudėtingas uždavinys tyrėjui. Apibenrinti esminių pažeidžiamumų valdymo gerinimo faktoriai pateikiami 16 paveiksle.



Šaltinis: *parengta autoriaus*

16 pav. *Esminių pažeidžiamumų valdymas – ontologinė schema*

Kai matoma 16 paveiksle, atlikus ekspertų interviu buvo identifikuotos trys pagrindinės esminių pažeidžiamumų valdymo gerinimo faktorių kategorijos: kognityviniai, valdymo, technologiniai. Apibendrinant valdymo faktorius, kurių buvo išskirta gausiausiai, pažymėtina, kad jų esmę sudaro suvokimo apie kritinius elementus, procesų kritiškumą, jų tarpusavio sąsajų ieškojimas ir jų inventorizacija. Visa tai parodo poreikį kuo daugiau žinoti apie pažeidžiamumus iš jų svarbos organizacijoje ir jų tarpusavio priklausomybės perspektyvų. Ekspertai taip pat išskyrė nemažai technologinių faktorių, kurių vieni labiausiai akcentuotinų: centralizuotas sistemų valdymas ir pažeidžiamumų šalinimas prieš plėtrą, būtent šie faktoriai, kaip parodė E5 eksperto interviu, atskleidžia vienas aktualiausių šiuo metu viešojo sektoriaus organizacijose egzistuojančių saugumo valdymo problemų.

3.4. Adaptyvių gebėjimų ugdymas siekiant padidinti organizacijų kibernetinį atsparumą

Adaptyvių gebėjimų gerinimo faktoriai, egzistuojanti adaptavimosi procesų formavimo problematika. E3 ekspertas, atsakydamas į klausimus kokie būtų svarbiausi veiksmai

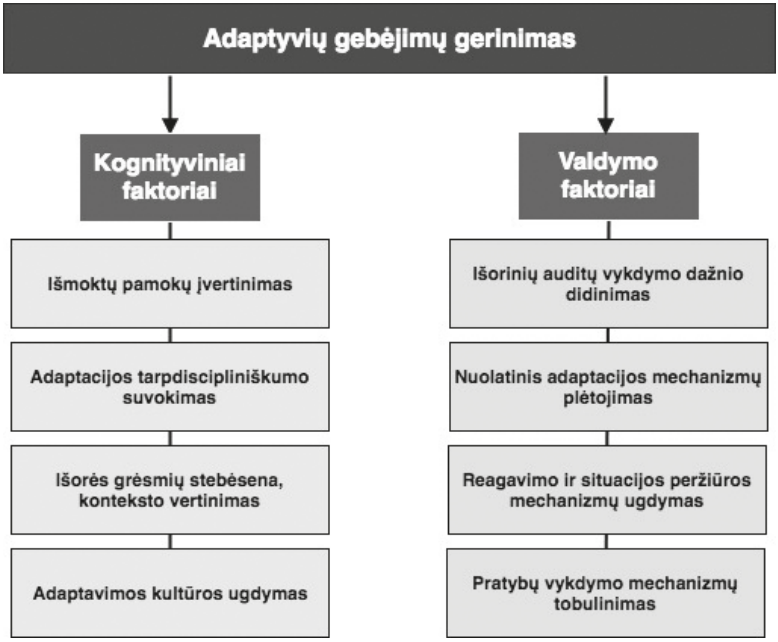
siekiant padidinti organizacijos adaptaciją: kaip geriausia būtų ugdyti adaptyvius gebėjimus, kad patyrus tą šoką organizacija būtų pasirengusi atsistatyti atgal; ar reikėtų proaktyviai kažkokius veiksmus daryti, ar daryti pratybas, padėsiančias pasirengti veikti krizinėmis sąlygomis; pažymėjo, kad kritinė dalis yra suvokti situaciją iki veiklos sutrikdymo kas atsparumo diagramos modelyje vaizduojama dalimi iki sistemos kritimo ir tuomet kai kritimas jau prasidėjo: „Adaptuotis krizėms, jeigu taip tiesiai pasakyti, aš kaip buvęs statutinis pareigūnas, sakyčiau, kad pasiekti [*adaptyvumą – aut.*], mažiau bijoti tų pavojų ir valdyti juos, pirmiausią tu turi išsigryninti va šitą liniją [sistemos gyvavimo dalį iki neigiamų veiksnių sąlygoto jos veiklos sutrikdymo, atvaizduojamą grafiniuose atsparumo modeliuose sistemos veiklos sutrikdymo [*lūžio tašku – aut.*], tik tada galima kalbėti kas bus, jeigu bus. Jei pas tave viskas nepatikimai sutvarkyta kasdieniniuose procesuose: procedūros, žmogiškieji ištekliai, įranga, tai kalbos negali būti. Bus kaladėlių principas – vienas nugriuvo ir nusinešė visus kitus.“ (E3, asmeninis interviu, 2017 m. liepos 21 d.). Analizuojant interviu metu ekspertų pateiktus atsakymus, ko gero, pačia pagrindine adaptavimosi priemone prie bet kokio masto grėsmių būtų galima laikyti E2 eksperto pateiktą siūlymą adaptuojantis nuolatinėms grėsmėms diegti sistemas, turinčias atsarginių kopijų darymo galimybes arba atskiras atsarginių kopijų sistemas: „Tiems dalykams pirmoje eilėje yra atsarginės kopijos. Tai jau dažnai įdiegta į sistemas pagal nutylėjimą. Jau senai suprasta, kad tu gali skaičiuoti, ruoštis, atsparumą savo didinti, bet atsitiks nenumatytas atvejis ir tavo sistema žlugs, arba kaip dabar Lietuvoje ir visame pasaulyje smarkiai paplitę koduojantys virusai, kurie užkoduoja visą informaciją kompiuteryje / serveryje ir prašo išpirkos. Tų atsarginių kopijų darymas jau parodo gyvenimiškai, kad padeda atsistatyti iš nenumatytų atvejų, neapskaičiuotų incidentų, kurių tu negali numatyti, bet jie vis tiek gali įvykti, tai vat atsarginių kopijų darymas tai viena priemonė.“ (E2, asmeninis interviu, 2017 m. liepos 14 d.). Kalbėdamas apie dviejų tipų adaptaciją skirtingo masto grėsmėms, E6 ekspertas pažymėjo, kad pakankamą dėmesį vertėtų skirti ir smulkiesiems įsilaužėliams: „Tų mažųjų nereikėtų nuvertinti, nes viskas prasideda nuo durų pabeldimo, o vėliau prasideda kitos atakos. Vis tiek pirmas būna tas surinkimas informacijos apie tinklą apie visus tinklo elementus, sekantis – prasideda atakos pagal surinktą informaciją ir pagal viešą informaciją.“ (E6, asmeninis interviu, 2017 m. liepos 26 d.). Kiek kitokias įžvalgas šiuo klausimu turėjo E1 ekspertas, kurio manymu, smulkios grėsmės turėtų būti valdomos automatizuotų priemonių pagalba ir į jas atkreipiamas dėmesys tik tada, kai jų statistiniai rodikliai peržengia nustatytas ribas: „Tie kurie yra lengvai atremiami ir suvaldomi automatiškai sistemų, į juos nereikėtų kreipti dėmesio labai smarkiai. Tu į juos žiūri statistikoje ir jei jų kiekis didėja, eksponentiškai, vietoj 1 ar 5 pasidarė šimtai, tai vadinasi blogai kažkas yra kažkur kitur, galbūt reikėtų pasitvarkyti kažką. Bet jei yra tie 5 incidentai, kuriuos vis kažkas suvaldo, sakykime 5 kintantys, nes jei 5 nuolatiniai ir kasdiena pasireiškia, reiškiasi pas tave yra spraga, kur jie ten 5 ateina, nes tada irgi turėtum pasižiūrėti iš principo. Bet jei vieną dieną atėjo 5 incidentai per paštą, kiti per kažkur kitur, bet jie susivaldė automatinėm priemonėm kaip ir nuo visko neapsisaugosi.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Diskutuojant apie krizinės situacijos pradžią, E3 ekspertas išreiškė nuomonę, kad ypač svarbu būti pasirengusiam kritimo momentui: „Dar kas svarbu, žiūrint šitą liniją, kai tik prasideda kritimas, tu turi žinoti kas pas tave dedas, žinoti kas pas tave dedas tai taip pat ir techninės

priemonės, ir išmanymas, ir pamainos kas pas tave vyksta. Ir tik tada tu gali pasakyti, kad mes jau krentam. O ne tada kai tau paskambina ir sako, žiūrėk kirvarpų prilindo.“ (E3, asmeninis interviu, 2017 m. liepos 21 d.). Kalbėdamas apie didžiąsias grėsmes, patenkančias į pažangių nuolatinių grėsmių (angl. *advanced persistent threat*) kategorijai E6 ekspertas pažymėjo, kad dėl jų aptikimo sudėtingumo jos kelia ypač didelius iššūkius, tad, eksperto manymu, čia reikėtų skirti pakankamą dėmesį techninėms priemonėms bei mokymams ir sutelkti pastangas į po incidentinę situacijos peržiūrą: „O tas *advanced persistent threat*, sunku juos aptikti, tikslius tuos APT. Dažniausiai tai tik post incident tyrimai ir padeda. Nes kai jau tam tikra ir žala būna ir tada kai pradeda aiškintis ir jau tam tikros pamokos yra išmokstamos, kad pavyzdžiui logų per mažai saugoma ir pan. Mokymai... Aišku mokymai, tai žinoma... Technologiniai sprendimai.“ (E6, asmeninis interviu, 2017 m. liepos 26 d.). Kalbėdamas apie adaptaciją nuolatinėms smulkioms atakoms E4 ekspertas pažymėjo, kad organizacija turėtų būti pasirengusi nuolatinėms grėsmėms pagal nutylėjimą iš anksto, o nenumatytoms situacijoms suvaldyti reikėtų pasikliauti veiklos tęstinumo mechanizmais bei bandyti pasirengti jiems per būtiniausių įgūdžių ugdymą mokymų ir pratybų metu: „Įprastom grėsmėm tu turi būti atsparus iš karto. Galbūt yra kažkokių išlygų dėl numatytų grėsmių, bet vėlgi, pas mus yra veiklos tęstinumo valdymas ir nenumatytų situacijų valdymo planų, o tos nenumatytos situacijos kaip tu jas suvaldysi?! Pagrindas tam yra, o kaip vat realiai būtų suvaldoma. Na, bandom organizuoti įvairius išbandymus, kartais ir pratybas bandom organizuoti. Niekas nėra apsaugotas nuo nenumatytų situacijų.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.). Atsakydamas į klausimus: kokios egzistuoja priemonės adaptuotis prie tokių netikėtų ir neplanuotų išpuolių, nestandartinių situacijų kibernetinio saugumo srityje; kaip valdyti tokias situacijas kuomet dėl atakos netenkama tam tikros sistemos dalies ar visos sistemos, E5 ekspertas pažymėjo, kad nepaisant didžiulio vidinio pasipriešinimo dėl sugaištamo laiko, žmogiškųjų resursų trūkumo efektyviausia priemonė yra – pratybos: „Pratybos, ir labai dažnai nerandama tam laiko, nes pratybos laikomos laiko gaišimu. Administratorių laikas yra aukso vertės, o kaip tik pratybos daugiausia jo ir sunaudoja. Tai vidinis pasipriešinimas didelis būna, įskaitant ir tuos pačius administratorius, netgi suvokiančių jų naudą, visgi tai yra darbo laiko sutrukdymas. Vis tik tai užtrunka ir jiem patiem darbų susikaupia. Tai dabar pratybas NKSC taip jau ruošiasi kasmet organizuoti. Pati organizacija taip pat tą turi daryti. Kritinės infrastruktūros – kasmet. Sunkiai vyksta šis procesas, kaip sakau: kol kas dar tai priimama kaip gaišinimas.“ (E5, asmeninis interviu, 2017 m. liepos 24 d.). Pratybų naudą pripažino ir E2 ekspertas bei akcentavo, kad būtina rengti ir atsistatymo iš atsarginių kopijų pratybas: „Tos pačios pratybos atsistatyti iš tų atsarginių kopijų, nes dažnai būna, iš praktikos susidūręs – daromos atsarginės kopijos kai tik įvyksta toks incidentas – užkoduoja kompiuterius, tai galvoja: ‘O! Mes gi darome atsargines kopijas, nieko mums baisaus’ ir pabando atsistatyti, ir nieko neišeina, pasirodo, kad neįsirašė kažkur ar baigėsi atmintis atsarginių kopijų sistemoje.“ (E2, asmeninis interviu, 2017 m. liepos 14 d.). E3 ekspertas taip pat pritarė pratyboms bei pasiūlė papildomą priemonę – vidinius ir išorinius auditus, įvardindamas tai kaip būdą nustatyti galimus neatitikimus sistemose: „Būti įsitikinusiam, kad tą dalyką pasiekti, tai va kaip minėjote, pasaulinė praktika organizuoti pratybas, t.y., kad pasižiūrėti, kad pas tave viskas veikia procedūriškai, žmonės *available* [*pasiekiami esant reikalui – aut.*] ir techninė įranga tikrai

daro tai ką, ką tavo „*adminai*“ arba tavo personalas sako, kad ji daro. Ir antras toks dalykas – sisteminiai auditai. Trečiųjų šalių. Išorinia. Nes nepažįstų nei vieno „*admino*“ nei vienos kompanijos kur nebūtų kažkokių skylių, to skylės atsiranda ir dėl žmogiškojo faktoriaus, dėl procedūrų netobulų, dėl visko. Bet taip, kad jau taip sulopyta viskas ir nei vienos skylės – taip nėra.“ (E3, asmeninis interviu, 2017 m. liepos 21 d.). Diskutuojant iš adaptyvumo perspektyvos, bandant įvertinti dabartinę saugumo būklę, suformuotas teiginys, kad, ko gero, incidentų skaičius auga, o visas kibernetinio saugumo sektorius smarkiai atsilieka, o kai kurių tyrėjų nuomone ir „mina atgal“. Atsakydamas į šį teiginį E4 ekspertas pastebėjo, kad puolančioji pusė dažniausiai išlaiko iniciatyvą bei pažymėjo, kad čia sudėtingą būtų kažką pakeisti, tad belieka tik racionaliai skirstyti resursus gynybai, neskiriant jų neapibrėžtoms grėsmėms: „Nežinau, ar mina atgal. Senai pastebėta, kad tokiose situacijose atakuojanti pusė turi iniciatyvą, tai čia mes ne išimtis ir vargu ar galim čia kažką padaryti. Leisti pinigus ir išteklius, ty. gintis nuo to kas dar nepuola kartais ir neefektyvu yra.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.). E5 ekspertas pastebėjo, kad vertėtų atsargiai vertinti statistinius rodiklius, nes jie dažnai parodo ne augančias grėsmes, o didėjantį jų aptikimo potencialą: „Kita vertus žiūrėkite atsargiai į statistiką, nes dalis to augimo nerodo atakų skaičiaus didėjimo, o rodo gebėjimus jas aptikti. Jų gerėjimą, techninės įrangos atakoms aptikti ir nustatyti gerinimą, o ne pačių atakų mastą. Netgi RRT, kur rodo ženklų augimą, šiek tiek jį reikėtų mažinti atsižvelgiant į technines priemones, kurios leidžia aptikti jų daugiau, t.y. kas buvo latentiška, dabar jau matoma, bet tai nereiškia, kad tokiais mastais išaugo. Aš manau, kad tas augimas yra sklandus, tolygus, o ne toks šuolinis. Kuo geriau matome, tuo daugiau ir pastebime.“ (E5, asmeninis interviu, 2017 m. liepos 24 d.). Plėtojant diskusiją apie pažangias nuolatines grėsmes E6 ekspertas pažymėjo, kad dėl jų sudėtingumo ir imlumo resursams reikalinga ypatinga atakuojančiųjų motyvacija, tai nėra spontaniški išpuoliai, tad adaptacijos objektui tokioje situacijoje būtina išmokti vykdyti veiklą šių grėsmių akivaizdoje: „Atakos staigiai neprasidės. Atakos dažniausiai jau būna pasiruošta keli mėnesiai tos APT. Nes APT padaryti reikia labai daug resursų. Ir tai turi būt motyvacija ją vykdyti, nes daug resursų, daug kainuos ir ją ruošiama pusę metų, nes reikia surinkti duomenis, surenki duomenis apie tinklą, negali rinkti labai greitai, turi iš lėto, kad tavęs neidentifikuotų, vis tiek žvalgybą vykdai viešuose šaltiniuose. Tada reikia turėt ir exploitą, kuris būtų nežinomas, *zero day*. Tada ir veiksminga, o kitais atvejais... Na aišku, jei pasitikrinai ir matai, kad ten windows XP, tai gali bandyt per žmogų paduot. Kiekvienu atveju skirtingai, Stuxnet atveju, tai va, ten prieš du mėnesius buvo užvaldyta. tas pats Black energy atvejis, buvo užvaldytos prieš du mėnesius sistemos, tik tada prieš tas kalėdines šventes paleido startą. Tai viskas iš anksto būna, ne taip kaip per filmus tą patį vakarą. Pakšt ir viskas griūna... Tai trunka ilgą procesą.“ (E6, asmeninis interviu, 2017 m. liepos 26 d.). Vėlgi, atsižvelgiant į sudėtingą pasirengimą tokioms atakoms, be būtinų technologinių sprendimų, kaip ir kitose atsparumo plėtojimo subkategorijose, būtina atkreipti dėmesį į darbuotojų įgūdžių ugdymą: „Žmogus sėdintis prie visos sistemos, jei pati protingiausia sistema, o žmogus be kompetencijos tai nieko iš to nebus. Tai tas žmogus irgi turi žinot ką turi daryt su tom sistemom ir ką daryt su tais duomenimis.“ (E6, asmeninis interviu, 2017 m. liepos 26 d.). E1 ekspertas kalbėdamas pažymėjo, kad kritiniai elementai atsparumui iš adaptacijos grėsmėms perspektyvos yra kibernetinio saugumo situacijos analizė ir

išmoktos pamokos: „Būtent atsparumui kritinės dalys: prevenciniai veiksmai, analizė ir būtent išmoktos pamokos. Apie ką šneka tie patys ISO standartai. Būtina priimti gerinimo veiksmus, visos gerosios praktikos apie tai šneka, kad būtų gerinimo veiksmai, kartais tai gali būti darbuotojų švietimas, kartais techninių priemonių pakonfigūravimas." (E1, asmeninis interviu, 2017 m. liepos 11 d.). Situacijos peržiūrą po incidento kaip efektyvią adaptacijos grėsmėms priemonę įvertino ir E4 ekspertas, pažymėdamas, kad tokios veiklos yra reglamentuotos teisės aktuose ir šiuo metu jau yra vykdomos: „Taip, turėtų būti tęsiama. Po tokių vat stambių incidentų numatytas: t.y. atstatomos veiklos pirmoje eilėje, bet visgi tas išmoktas pamokas taip pat analizuojame. Tai net kibernetinio saugumo įstatyme tokia nuostata yra." (E4, asmeninis interviu, 2017 m. liepos 24 d.). Papildydamas teiginius apie išmoktų pamokų svarbą E1 ekspertas pažymėjo proaktyvumo poreikį ir pagrindinių incidento priežasčių (angl. root cause) analizę: „Reikėtų pradėti žiūrėti anksčiau... Taip, yra incidentų šalinimo ciklas, bet yra labai praleidžiamas esminis dalykas, taip – patyrė incidentą, stengiasi jį suvaldyti, atstatyti veiklą, bet niekas nesigilina į kaip jis atsirado: ar jis atsirado dėl to, kad kažkas gavo laišką, ar jis atsirado, kad kažkur sistemoje yra pažeidžiamumai, ar atsirado dėl to, kad tinkle kažkokia spraga yra. Kol tu šalinsi tik incidentus ir atstatinėsi veiklą, nežiūrėdamas į pradžia į kilmę ir paskui sekantis žingsnis išmoktos pamokos, tol ir kovosi. Tu pradedi iš pradžių kovoti su vienu priešu, o baigiasi, kad kovoji su mase ir nebespėji, o tave per tas pačias vietas vis lauš. Kol tu nepradedi nuo pačios grandinės pradžios analizės, vertinimo ir nepraeini viso ciklo iki išmoktų pamokų kas yra pabaigoje, tol ir bus blogai, priklausomai nuo incidento kilmės, išmoktos pamokos parodo kas buvo incidento šaltinis." (E1, asmeninis interviu, 2017 m. liepos 11 d.). E2 ekspertas pažymėjo, kad dalis adaptacijos mechanizmų turėtų atsispindėti veiklos tęstinumo planuose, numatant scenarijus, apibrėžiančius visas galimas veiklos kryptis krizinių situacijų atvejais: „Verslo tęstinumo planai, t.y. numatyti patį blogiausią scenarijų ir ką daryti, daryti rezervinį biudžetą nenumatytiems atvejams. Tarkim, „miršta" visi kompiuteriai, negali atstatyti, *policy* [*politika – aut.*] tau neleidžia mokėti išpirkos hakeriams, teroristams už duomenis, tu turi atsarginius kompiuterius, iš kurių atsistatai ir darai savo įmonės veiklą, arba turėti į cloudus/į debesis išneštus savo servisus, kažkokius kritinius, kad jeigu tavo organizaciją, kad ir fiziškai užtvindė, tu gali vis tiek aptarnauti savo verslą toliau iš rezervinių arba debesų kompiuterijos paslaugų." (E2, asmeninis interviu, 2017 m. liepos 14 d.). E6 pažymėjo ir išorės veiksnių stebėseną ir organizacinės sistemos adaptacijos prie kibernetinių grėsmių konteksto būtinybę: „Bendras kontekstas tam tikras. Vat išėjo, buvo paviešinta, kad buvo tie duomenys exploitų, NSA. Ir jie gi jau buvo kalbama kokią spragą išnaudoja. Tai jeigu tu esi saugos specialistas tai jau gali sunerimt 445 poprtą, gal reik užsidaryti. Atsinaujinti, nes kovo mėn. išėjo updateas Windows OS. Daug veiklos, bet žmogui vienam gal net kartais sunku viską aprėpti. Aišku būna kai kurios korporacijos turi CERT'ų padalinius, kurie užtikrina incidentų tyrimą ir kitų saugos priemonių formavimą." (E6, asmeninis interviu, 2017 m. liepos 26 d.). E5 kalbėdamas apie bendras adaptyvumo tendencijas pažymėjo, kad labiau būdinga mūsų organizacijoms yra reaguoti nei adaptuotis ar pasirengti. Eksperto nuomone po incidentinių įvykių peržiūra taip pat turėtų būti tobulinami: „Visgi tendencija yra jau reaguoti. Daugiau negu prevenciškai pasiruošti ir gebėjimai to reagavimo ugdomi pakankamai. Vat pasirengimo, pradinio to atsparumo – ne taip. O

prasčiausia su išmoktom pamokom, jų užfiksavimu, sistemų veiklos atkūrimo specifika. Va čia, manau, tikrai yra kur tobulėti.“ (E5, asmeninis interviu, 2017 m. liepos 24 d.). Apibenrinti adaptyvių gebėjimų gerinimo faktoriai pateikiami 17 paveiksle.



Šaltinis: *parengta autoriaus*

17 pav. *Adaptyvių gebėjimų gerinimas – ontologinė schema*

Kaip matoma 17 paveiksle, adaptyvių gebėjimų gerinimo srityje galima išskirti dvi kategorijas, apimančias kognityvinius ir valdymo faktorius. Nors šios kategorijos faktorių yra mažiau nei kitų atsparumo gerinimo elementų, vertėtų pastebėti, kad daugelis jų ekspertų laikomi svarbiais, siekiant padidinti organizacijos atsparumą kibernetinėms grėsmėms. Iš abiejų kategorijų vertėtų išskirti: adaptavimosi kultūros ugdymą, išorės grėsmių ir išmoktų pamokų vertinimą, pratybų vykdymą.

3.5. Sistemos lankstumo gerinimas siekiant padidinti kibernetinį atsparumą

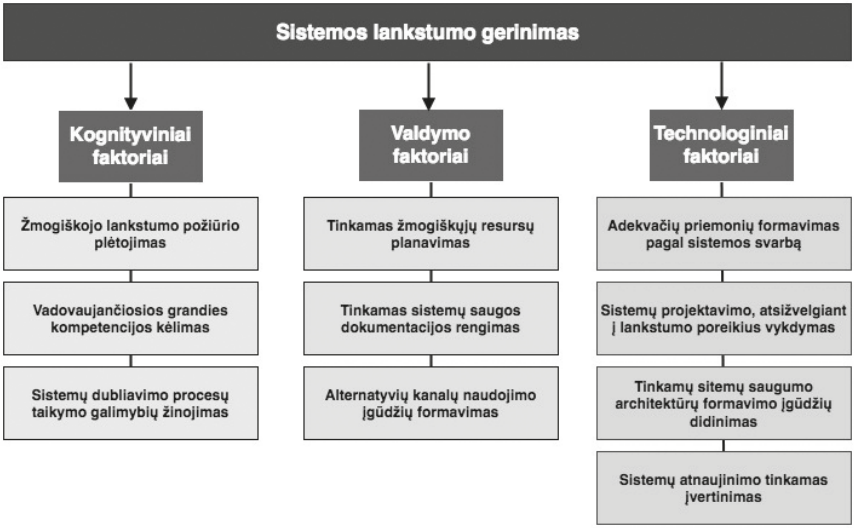
Esminiai sistemos lankstumo formavimo faktoriai. Diskutuojant apie lankstų sistemos perprojektavimą, reaguojant į situacijos dinamiką, E1 ekspertas pažymėjo, kad visi veiklos procesai turėtų būti derinami pagal situaciją ir neturėtų būti taip, kad IT sauga trukdytų verslo procesams ir juos apsunkintų: „Tiek dėl IT visos atsiradimo tobulėjimo, tiek dėl saugos sprendimų, dažnai sauga tam tikrus procesus prailgina, kaip bebūtų, ji kartais trukdo verslui, todėl būtina rasti aukso vidurį tarp saugos ir veiklos. Ir visi standartai, gerosios praktikos būtent ir sako, kad aukso viduriuko radimas yra labai svarbus. Sauga turi

tapti verslo dedamoji, o ne trukdymu.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). E4 ekspertas pastebėjo, kad, kaip praktika rodo, sistema gali būti pakankamai lanksti, tačiau dažniausiai tinkamai pasirengę, organizuoti nusikaltėliai ją vis tiek nulaužia, todėl reikėtų vertinti nebent situacijas, kai atakuojantieji pabando sutrikdyti sistemų veikimą, tačiau galiausiai atsisako savo pradinių užmojų: „Rimti puolėjai, kol jie nepasiekia savo tikslo, tol jie neatstoja. Tai būk lankstus kiek nori, vis tiek jie tave nulauš. [...] Tai vat tai – darykit ką norit, o poveikio nebus. Taip tai yra galima strategija tokia, kad mus griauna, mes atsistatom ir veikiam toliau. Ir kiek norit, tiek mes tą darysim. Tik aš maniau, kad čia labiau būtų susiję, kad mus palankstysite ir atstosit [...] kažkuriuo momentu gali pasakyti: ‘ai nepavyko, galim susirast kažką kitą. ’ Būtent, tas *advanced persistant threat* tai ir yra – jisai turi savo tikslą ir jis nesustos kol jo nepasieks.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.). Paklaustas apie galimus lankstumą gerinančius sprendimus, E6 ekspertas pažymėjo, kad egzistuoja aibė būdų, kaip tai organizuoti, tačiau vienas esminių komponentų sistemos lankstumo užtikrinimo procesuose – žmogiškasis faktorius. Ir kol egzistuoja silpnosios grandys, tokios kaip žmonės, motyvuoti įsilaužėliai ras būdų kaip sistemą nulaužti: „Kaip praktika rodo nuo senų laikų – galiausiai kažkas bet kokią saugumo priemonę nulaužia. Bet galima išskirti sluoksnius tam tikrus, kaip svogūną. Bet vis tiek tai vienam tinkle, iš to tinklo darys kitą ataką, kaip tos advanced persistent threat atakos taip ir vyksta. Ir galiausiai pakliūna iki kokių SCADA sistemų. Nes lupa lupa tą svogūną ir vis tiek pakliūsi tenai. Ypač kai didelė organizacija tai kartais sunku ir suvaldyti, tiek technologinius resursus, tiek žmogiškuosius.“ (E6, asmeninis interviu, 2017 m. liepos 26 d.). Sistemos lankstumo sąsają su personalu pažymi ir E3 ekspertas, ypač akcentuodamas sistemos uždavinių išgryninimą bei pažymį būtinybę atsižvelgti į lankstumą pradinėse sistemos formavimo stadijose: projektavimo, pirkimo, diegimo metu: „Sistemos lankstumas yra tiesiogiai susijęs su tuo pačiu personalu. Ne tik Lietuvoje, bet Lietuvoje ypatingai aktuali problema yra ta, kad aš moku dirbti tik su *MS Windows* operacine sistema ir pas mane visos sistemos *MS Windows*, nes „*next*, *next*, *next*, *finish*...“ [*ironizuojama* Microsoft Windows *vartotojo sąsaja – aut.*]. Tad pradedant sistemos projektavimu, pirkimu, diegimu labai prisideda žmogiškasis faktorius, kad: ‘aš moku, mes turim specialistus ir mes galim padaryti šitom priemonėm.’ Nors geroji praktika ir tie, kas supranta tą lankstumą kaip jis turi būti, tai pirmiausia tu susiformuoji uždavinį ką tau reikia padaryti. Ką sistema, ką tinklas, ką jis turi pasiekti, kokie rezultatai jo turi būti. Ką jis turi užtikrinti, kaip jis turi veikti ir tik po to daryti jo architektūrą, kuri įranga galėtų būti naudojama. Jei pagal uždavinius turi būti dvi skirtingos sistemos. Orlaiviai turi tris ir gamintos skirtingų gamintojų privalo būti. Tik tada kai tu apsirašai ko tu nori tau ateina tas sistemos lankstumas.“ (E3, asmeninis interviu, 2017 m. liepos 21 d.). Išankstinį lankstumo numatymą akcentavo ir E7 ekspertas, kuris atkreipė dėmesį, kad bandymas pasiekti lankstumą atnaujinamose, iš prigimties statiškose sistemose gali duoti neigiamų rezultatų, todėl, norint sukurti lanksčias sistemas, reikėtų jas kurti iš pagrindų, nes, priešingu atveju, rigidiškai sistemai pereiti iš statiškos būsenos į lanksčią bei suformuotą moduliais gali būti pernelyg sudėtinga: „Lankstumas turėtų būti jau numatytas pradžioj prieš kuriant sistemą. Ir gal jei tu nori lankstumo, iš naujo reikėtų naują sistemą padaryti, pakeisti, netgi sakyčiau ne ant to kas yra pastatyta dar bandyti prilipdyti naujus gabaliukus, o bandyti pereidinėti prie pilnai atnaujintos sistemos. Nes modulinė sistema tai

yra gerai, bet ji turi būti tam pritaikyta, o ne galvoti apie statišką sistemą ir iš tos statiškumo pereiti į lankstumą, modulinius dalykus." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Kalbėdami apie sistemų organizavimą moduliais ekspertai turi skirtingų įžvalgų, dalis pastebi, kad praktinėse situacijose modulinis principas yra pakankamai sudėtingai įgyvendinama bei nepageidaujama sistemos būsena. Visa tai yra dėl potencialios įrenginių įvairovės, kuri apsunkina sistemos ir jos komponentų tiekėjų valdymo procesus. Tokios sistemos palaikymui reikalingi skirtingą kompetenciją turintys specialistai, vėl gi reikalingas įdirbis tokias sistemas projektuojant, nes padarius klaidų iš skirtingų komponentų „suklijuota sistema" būtent ir plyšta toje vietoje: „Praktikoje įvairovė yra blogai, kai tu dirbi pagal standartą, tu gali centralizuotai valdyti visus įrenginius. Tu turi *Cisco* centrinį serverį tu atnaujinimus „pūti" konfigūruoji viską iš vienos pusės, kai bus didelė maišalynė tų įrenginių, nekalbu apie du tiekėjus, bet tarkim bus HP, *Cisco*, dar kažkas. Tada tau reik skirtingų specialistų, tie specialistai turės būti vienodo lygio supratimo, gebėti tuos pačius dalykus. Arba vienas žmogus turi būti universalus, bet tokį žmogų išlaikyti turėsi ženkliai didesnę pinigų sumą mokėti." (E1, asmeninis interviu, 2017 m. liepos 11 d.); „Skirtingų komponentų taikymas nėra labai gerai, bent jau man kiek teko susidurti. Visų pirma, reikėtų apgalvoti kai tu ją projektuoji, o dažniausiai būna kaip – ne tada galvoja kai projektuoja, o kada jau reikia daryt kažką, naujo įvedinėt ir tada bandoma prie senos sistemos klijuoti. Ir va tas vat suklijavimas, dažniausiai ten ir plyšta per tą vietą." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Be to, tai reikalauja papildomų finansinių ir veiklos resursų: „Kai turi vieną vendorių [*tiekėją – aut.*] ir jo įrenginius, tu turi galimybę viską automatizuoti ir sugaišti mažiau laiko. Jei būtų tvarkingai keliais lygiais prižiūrimi visi įrenginiai, tuomet saugumas būtų geresnis, bet tikėtina, kad bus praleista kažkuriam lygmenį kažkas, ir būtent dėl to tas saugumas ir nukentės, ir nukenčia dažniausiai būtent dėl to. Kažkas tiesiog neatlieka savo darbo, administratorius buvo silpnesnis su tais įrenginiais. Bet čia kalbant apie tinklo įrangą, jei apie serverius, jokio skirtumo ar ten sukasi HP ar *Dell*'as. Jie savyje atskirai segmentuoti, atskirtos aplinkos, kad nebūtų tame pačiame serveryje, sukurta DMZ zona, vidinės sistemos." (E1, asmeninis interviu, 2017 m. liepos 11 d.). Priešingai E1 ir E7 ekspertų nuomonėms, E5 ekspertas pažymėjo, kad sistemos formavimas moduliais būtų pakankamai efektyvi priemonė, taikytina su alternatyvaus planavimo mechanizmais: „Modulinis sprendimas, aš manau, efektyvus tikrai būtų [...] ir planas B. Jei neveikia kažkuris, tai jo funkcionalumas gali būti dubliuotas, įskaitant netgi dokumentinį dubliavimą ir perėjimą prie popierinio valdymo. Tai vis dar veikia [*popierinis valdymas – aut.*]. Praktikoje buvo sutrikimų sistemų pasienio ruože ir padarėm išvadą, kad labai sėkmingai pereinama prie ne IT sprendimų tikrinimo, o tiesiog fiziškai. Tai vat vienas iš lankstaus sprendimo variantų." (E5, asmeninis interviu, 2017 m. liepos 24 d.). Ekspertas taip pat akcentavo alternatyvaus ryšio kanalų taikymą, į kuriuos, esant poreikiui, visuomet galima būtų nukreipti ryšio srautus: „Taip, tas turėtų būti. Plačiąja prasme apie komunikacijas imant, netgi apima galimybę naudotis alternatyviu tinklu. Kaip paslauga kritinei infrastruktūrai, t.y. turėti sutartis, esant kritinei ir krizinei situacijai naudotis alternatyviu tinklu kritinei infrastruktūrai. Jeigu įprastinio paslaugos teikėjo paslaugos yra sutrikdomos ir yra atkertama, kad ir dabartinio populiaraus DDoSo atakų. Šitą sprendimą sėkmingai naudoja LT banko IT padalinys, turi sutartį ir operatyviai gali persijungti." (E5, asmeninis interviu, 2017 m. liepos 24 d.).

Alternatyvių – dvigubų sistemų taikymą akcentavo ir E3 ekspertas, iliustruodamas savo teiginius kritinių sistemų dubliavimo praktiniais pavyzdžiais: „Yra dvigubos sistemos, visur mažiausiai kurios AIRAC ciklas vadinamas, kurios keičiasi kas 40 parų, t.y. veikia viena sistema, kuri veikia *standby*, ne failover pagrindu. Tuomet viena sistema po 40 dienų išjungiama, keliama atsarginė ir tada jau praeina. Nes kaip rodo patirtis, jei 2–3 metus stovi *standby* ir ji neveikia, tai galbūt ten kažkas sugedę. Tad taip mes užtikriname funkcionalumą, kad viena ir kita sistema yra gyvos. Viena išjungiama, kita įjungiama. Tai nevyksta automatiškai, tai turi padaryti žmonės." (E3, asmeninis interviu, 2017 m. liepos 21 d.) Kalbėdamas apie sistemų dubliavimą, E1 ekspertas pažymėjo, kad iš racionalių ir adekvačių saugos priemonių taikymo perspektyvos labai svarbus yra sistemos kritiškumo nustatymo aspektas: „Jei sistema yra kritinė, turėtų būti dubliuotas veikimas, sustoja veikti duomenų centras, persijungia į kitą. Kitom sistemoms užtenka, kad būtų atsarginės kopijos, kad sistemą būtų galima prikelti per valandą, per 4 valandas ar per dieną. SLA, RTO, RPO – kad tu žinotum kiek tau ta sistema yra svarbi ir kiek iš jos norėti. Paimkime kokią dokumentų valdymo sistemą, kaip pavyzdį. Vieniems ji be galo svarbi, ten viskas yra sąskaitos, sutartys. O kitoje įmonėje ji naudojama tik gautų dokumentų registravimui ir vieną dieną jei ji neveiks tai nieko, sekretorė suregistruos po savaitės. Tad vienur ji gali aukštesnio patikimumo būti, o kitur veikti paprasčiau.Vienur ta sistema gali būti prieinama iš išorės, kitur – ne." (E1, asmeninis interviu, 2017 m. liepos 11 d.). Papildydamas savo teiginius apie sistemos lankstumo principų įdiegimą sistemos projektavimo etapuose E7 ekspertas pažymėjo, kad projektavimas turėtų būti vykdomas remiantis į egzistuojantį poreikį, o ne į bandymą panaudoti turimus nereikalingus komponentus: „Projektuojant, o *a priori*, kad: 'aš turiu ir man reikia, kad šitas būtų panaudota,' nesvarbu, kad tai netinka. Dažniausiai kas pasako tai – ne informacinių technologijų specialistas, o vadovas, nes: 'kitkam nėra pinigų, panaudokite ką mes turime.' Tai vat kai pas jį atsiranda supratimas, kad jis turi specialistų paklausyti, o jeigu tas sako, kad netinka, tai nereikia spausti, kad naudoti." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Kalbant apie sistemos pertvarkymą atakų metu, E1 eksperto buvo prašoma pateikti įžvalgų ar tais atvejais jeigu sistema konkrečiu metu laike jau yra atakuojama, ar dar galima bandyti ją pertvarkyti, ar tai yra įmanoma? Šiuo klausimu E1 pateikė neigiamą atsakymą ir pažymėjo, kad priklausomai nuo grėsmių taikytinos nebent tam tikrų sistemos komponentų izoliavimo priemonės: „Jau nebe. Žiūrint ką tu nori padaryti, pirmiausia jeigu tavo sistema yra atakuojama, kokiu tai principu daroma. Jei virusas, tu gali izoliuoti tą sistemą iš išorės ir tada viduje aiškintis – kas ten per virusas, kodas kaip jis veikia. Jei esi atakuojamas iš išorės, be įsibrovimų į vidų, pvz. DDoS, tuomet tu atskirinėji perimetrą, nes žinai, kad pas tave viskas bus gerai. Bet kitos būna priemonės, kad tu gali nežinoti ar pas tave nieko nėra, tu matai, kad pas tave srautas vaikšto. Ir tu nesupranti iš kur tas srautas. Kai tu atkirsi perimetrą, tu prarasi šaltinį analizei, todėl tu turi pasidaryti kloną, dėti į *sandboxą* ir žaisti bei žiūrėti kas vyksta. Nes jei tu pradėsi nagrinėti sistemą neperdėjęs visko į kitą sistemą, tu prarandi visą analizės etapą ir po savaitės vėl gali turėti tą patį." (E1, asmeninis interviu, 2017 m. liepos 11 d.).

Apibenrinti sistemos lankstumo gerinimo faktoriai pateikiami 18 paveiksle.



Šaltinis: *parengta autoriaus*

18 pav. *Sistemos lankstumo gerinimas – ontologinė schema*

Sistemos lankstumo gerinimą apima trijų kategorijų faktoriai, iš kurių dažniausiai naudojamas – technologinis. Vertėtų išskirti technologinį faktorių, kurį dauguma ekspertų pažymėjo kaip svarbiausią, t.y. sistemų projektavimą, atsižvelgiant į lankstumo poreikius, vykdymą. Kalbant apie valdymo faktorius, vertėtų pažymėti, kad po interviu su ekspertais, ypač akcentuotinas alternatyvių kanalų naudojimo įgūdžių formavimas. Iš kognityvinių faktorių perspektyvos, išskirtini vadovaujančios grandies kompetencijos kėlimas ir žmogiškojo lankstumo požiūrio plėtojimas.

3.6. Reakcijos į atakas gerinimas siekiant padidinti kibernetinį atsparumą

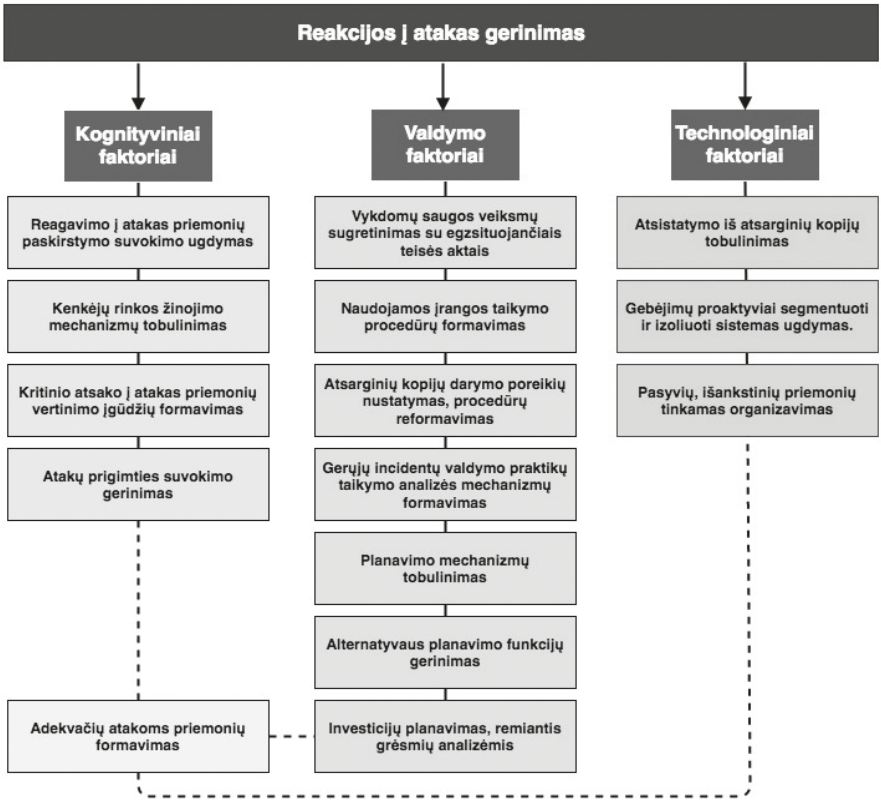
Reakcijos į atakas gerinimo procesų esminiai faktoriai ir trukdžiai. Kalbėdamas apie reagavimo veiklų bendrą padėtį Lietuvos viešajame sektoriuje, E1 ekspertas pažymėjo, kad šiems procesams vykdyti yra suformuota pakankama teisinė bazė, paremta egzistuojančiomis kitų šalių praktikomis, tačiau kaip ir daugelyje kitų sričių egzistuoja tikimybė, kad kai kurios institucijos gali netinkamai ją vykdyti: „Yra Kibernetinio saugumo įstatymas, kibernetinio saugumo organizaciniai reikalavimai ir juose ten yra kas turi būti įtraukiama ir tas pats Nacionalinis kibernetinių incidentų valdymo planas, bendrai tos gairės kaip tas viskas daroma, kadangi pats dalyvavau rengiant tai ten kaip ir sudėliotos geros praktikos, nes ten buvo paimta ir kanadiečių, ir olandų. Iš tų pačių standartų ką reikia daryti, ką pasižiūrėti, kokius klausimus sau atsakyti, kad sėkmingai tą padarytum, kad žinotum, ką vėliau reikia daryti, kad tau tas pagelbėtų, bet kaip tas praktiškai veikia, vienose įmonėse viskas veikia, viskas puiku – incidentas užregistruojamas ir prasisuka visas ciklas, ir paskui pabaigoje aiškios pamokos, aišku kas ką padaro, o kitose taip ir lieka – planas sau, realūs

darbai sau, viskas kas sudėliota popieriuje turi atsirasti ir gyvenime.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Plėtojant diskusiją apie reagavimo veiklas, E6 eksperto nuomone, šių veiklų organizavimas, apimantis teisines, organizacines ir technines priemones turi būti išdėstytas saugumo politikoje: „Pirmas dokumentas turi būti saugumo politika organizacijoje, kuri apibrėžtų tiek reagavimą į incidentus tai turi būti kontaktai, telefonai, kas ten yra 24h valandas per parą dirbantys žmonės. Tas žmogiškasis resursas. Jei nėra, tai yra automatizacijos sistemos. Pas mus yra alertavimas, smsai, emailai. Žmogui gali nebūti vietoje, bet visada pasiekiamas telefonu. Žinutės eitų apie anomalijas tinkle. Sistemos turi būti IDSai dar kažkas, jos fiksuoja ir ta informacija keliauja atitinkamam žmogui.“ (E6, asmeninis interviu, 2017 m. liepos 26 d.). Be to, ekspertas pažymėjo tinkamam atsakui reikalingą adekvataus situacijos vertinimo būtinybę bei alternatyvų planavimą: „Turi būti stebėsenos sistemos, kad identifikuotų. Kai kurie resursai turi būti išskirti, kad DdoSo atveju išsiaiškinti ar tau DdoSas kenkia ar nekenkia. Jei ne, užsidarai nuo užsienio ir LT rinkoje dirbi ir tiek. Jei kenkia, tuomet turi būti tam tikros priemonės išmesti tuos CDN‘inius tinklus ir visi kiti, arba turėti apsaugas. Su apsaugom yra sudėtinga, jei nesi paslaugos teikėjas, tuomet neturi tokios didelio srauto, kad tau neužkištų ryšio, tai jau geriau išskirstyti tuos resursus. Čia irgi saugumo politikoje turi apsibrėžti kas pas tave, kokios sistemos, žmonės, paslaugos, čia galima sakyti yra gynybos planas. Amerikoje tai labai populiaru, ten planas A, jei tai atsitinka, planas B... Vis tiek turi būti numatyta tas iš dalies. Jei tu nebuvai iš anksto to pasidaręs, tai reakcija į ataką bus labai ilga ir nebebus prasmės, paatakuos 2 dienas ir kol tu susigriebsi ką pasidaryti. Kai susiplanuoji, viską jau žinai, maždaug galimas rizikas kokios bus: DdoS’as dar ten kas.“ (E6, asmeninis interviu, 2017 m. liepos 26 d.). Kalbėdamas apie reakcijos į atakas E4 ekspertas pastebėjo, kad atakų metu kritinė savybė yra reagavimo greitis: „Greitis turbūt svarbiausias faktorius, tai yra komunikacijos greitis, žinojimas, kad tave atakuoja. Sensoriai ar signalizacijos. Tai yra kuo greičiau aptikti ataką ir kuo greičiau į ją reaguoti. Aptinkama paprastai techninėmis priemonėmis, o reagavimas – žmogus turi įsitraukti ir, kad tie žmonės galėtų komunikuoti.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.). Apskritai reakcijos į atakas priemonių formavimas, atsižvelgiant į atakų įvairialypę prigimtį, yra ganėtinai sudėtingas reiškinys. Planavimas šioje srityje taip pat nėra lengvas, kaip pažymi E6 ekspertas, dėl nuolatinės grėsmių kaitos darosi neįmanoma atoveiksmių formuoti iš anksto: „Ganėtinai sudėtinga būtų tas atakas apsvarstyti. DdoS’as tai viskas aišku, o ką tu virusą? Na gali *ransomwarui* sakyti – turi būti *backup*’ai kiekvieną dieną, užpatchintos sistemos, SMB uždarytas. Šiuo atveju, šią dieną kalbant SMB turi būti uždarytas. Kitą dieną neaišku kas bus, kitas gal kažkas bus išnaudotas. SMB pavyzdžiui 445 portai, 137 iki 139 portai anksčiau provaideriai, ne LT, bet kitose šalyse blokuodavo jį tinkle. Čia buvo prieš 7 metus visi sakydavo: ‘kam jūs tai darot?’ Dabar vat – pūkšt. Vėl tas pats portas ir vėl jį išnaudoja. Paprasčiausia tais laikais tada plito, paskui niekas nebeplito. Kirminai buvo nebeefektyvūs *conflickeris* dar vienas iš tokių kirminų buvo. Paskui jų nebeliko, prasidėjo ransomwarų banga. O dabar va kažkas naujo – *ransomwaras* su kirminu.“ (E6, asmeninis interviu, 2017 m. liepos 26 d.). E3 ekspertas reakcijų į atakas veiklų kontekste išskyrė aibę kompleksinių priemonių: tinkamas stebėsenos ir apsaugos įrangos valdymas, tinkamas įgaliojimų vykdymas atakos metu ir kibernetinės ekspertizės atlikimą (angl. *cyber forensic*): „Pradedant žiūrėti, kaip tu gerai ir

teisingai valdai įrangą, ar tu žinai kas vyksta, monitoringo centrai. Ir toliau tau reikia tik procedūriškai atlikti veiksmus. O vat čia ir pats įdomumas, kurio LT yra tik keletas žmonių kurie supranta. Yra tokia sąvoka – „forensic", ty. surinkti įrodymus, kurie tiktų baudžiamajam persekiojimui arba kitoms procedūroms atlikti. T.y., tas žmogus, atėjęs prie įrangos, reaguoti jis turi automatiškai žinoti, ką jis gali daryti ir ko jis negali daryti. Tai aprašo *forensic*. *Forensic* mes turim žmonių, na keletą. Tau reikia kviesti ekspertus į vietą ar nereikia, viskas tai priklauso. Toliau yra įgaliojimai, kad tu gali išjungti. Aš klausiu: 'ar gali išjungti serverį?', sakau: 'eik, išjunk generaliniam direktoriui kompiuterį, pasakyk, kad jis apkrėstas virusais ir pasitikrink savo įgaliojimą.' 'Ne, direktoriui negalima.' Tai apie ką mes kalbame? T.y. tu būsi nedrąsus prisiimti atsakomybę už savo veiksmus. Bet, jei tu supranti pavojus, tau reikia daryti dabar, ne rytoj, nelaukti sprendimo. Paskui ten jau aiškinsis tu kaltas, nekaltas, bet tu turi užkardyti, turi suveikti prevencinė sistema. Bet čia Lietuvoje yra pakankamai „silpnai" šioje srityje." (E3, asmeninis interviu, 2017 m. liepos 21 d.). E7 ekspertas akcentavo reakcijos ir sistemos atstatymo greitį ir taip pat pažymėjo keletą priemonių, priskirtinų prie pasyviųjų kategorijos: veiklos reglamentavimą, sistemų decentralizaciją, anomalijų stebėsenos įrangą: „Atsistatymas sistemos, reakcijos laikas. Jeigu atakuoja gal dažniausiai net nematai, kad tave atakuoja. Ir čia jau yra jeigu tave jau dabar atakuoja, tai šaukštai po pietų. Gal decentralizacija sistemos didesnė, modulinės sistemos vėlgi, tvarkos kažkokios. Nes dažniausiai kaip būna, yra labai daug galbūt įrangos, bet kaip su ta įranga dirbti, na tvarkų kažkokių nėra." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). E3 eksperto pasiūlytos aktyvios priemonės apima sistemos parengtinį segmentavimą, kad, esant krizei galima būtų nukreipti srautą ir naudoti izoliuotas sistemos dalis: „Jeigu tai sistema yra, jos vertė yra didelė – tik dubliuota įranga. Kad tu galėtum atsijungti nuo išorės ir blokuoti, segmentuoti, jei tai yra didelės bendrovės – atjunginėti vos ne regionais, kad neplistų toliau po tavo visą tinklą. Vidinė apsauga, sensoriai viduje: anomalijoms tinklui, tinklo analizė tiesiog. Kodėl taip, kodėl kas čia vyksta ir kodėl apskritai vyksta? Kodėl tas aktyvumas padidėjo? Gal nieko blogo, gal kažkas failą didelį siunčiasi, o gal ir problema." (E3, asmeninis interviu, 2017 m. liepos 21 d.). Kalbant apie atsarginių kopijų darymą, E1 ekspertas pažymėjo, kad kritiškai yra svarbu parodyti atsarginių kopijų darymo svarbą ne IT ar saugos padaliniams, o likusiai organizacijos daliai: „Visas tas *backup*'o darymo, atstatymo, išbandymo visas procesas, kad žmogus, kuris daro backupus ir parodo verslui, kad tai yra padaroma: 'žiūrėkite, mes darom backupus jums nulėkė sistema, bet mes atstatėm iš naktinio *backup*'o versijos ir praradom tik tokią dalį duomenų, viskas veikia, viskas tvarkoj, galim dirbti, tik mums reikia susirinkti prarastus duomenis.' Dėl to ir yra RTO, RPO, kad įmonės įsivertintu, kiek duomenų gali prarasti ir per kiek laiko atsistatyti. Turi būti parodyta *backup*'o nauda, nes sumokės pinigus be garantijos, kad jiems atkurs. Nežinau kodėl žmonės tiki, čia vat ką skelbia, ir policija ypatingai, po visų atakų ir KSC ir RRT, kad nemokėkite tų pinigų, niekas tų duomenų jums negrąžins, o jei grąžins ar nepasiliko kopijos ir nepanaudos prieš jus, jei jums reik verslui, darykitės backupus patys." (E1, asmeninis interviu, 2017 m. liepos 11 d.). E4 ekspertas atsakydamas į klausimą ar atsarginių kopijų nedarymo priežastimi gali būti nepasitikėjimas jomis, pastebėjo, kad tai galbūt ne visuomet yra susiję su nepasitikėjimu, veikiau problema yra tame, kad atsarginėse kopijose esantys duomenys dažnai būna taip pat užšifruoti į jas neapdairiai nukopijuotų

kenkėjiškų šifruojančių programų: „Čia gal net ne pasitikėjimo klausimas, čia buvo: 'aš pažiūrėjau atsargines kopijas, o ten jau irgi viskas buvo užšifruota, padariau atsargines kopijas, kai jau tas viskas įvyko.' Čia daugiau klausimas buvo: kur tavo ankstesnės atsarginės kopijos, kur tavo mėnesinis ar metinis, gal bent ką gali atstatyti. Tai atsarginės kopijos, tai tradicinė saugos priemonė ir metodikų daug. Reikia laikytis rekomendacijų ir gerosios praktikos. Turėti atsargines kopijas kelių lygių, atitinkamai apsaugotas, kad niekas neprieitų, patikrinti, išbandyti laikas nuo laiko." (E4, asmeninis interviu, 2017 m. liepos 24 d.). E6 ekspertas taip pat pažymėjo, kad reikėtų nusimatyti, jog dalies duomenų nepavyks atstatyti iš atsarginių kopijų: „*Backup*'as – jau paskutinė stadija, kas tau gali išgelbėti, jei tu praradai duomenis. Aišku bus dalis tų prarastų duomenų. Juos reikia saugoti ir saugumo politikoje turi būti apibrėžta, kas kiek laiko ir kur jie turi būti saugomi. O kas moka tiem blogiečiams, praktika nėra gera, nes *Petyos* atveju sumokėjo 50 organizacijų, kurios nieko ir neatgavo. Aišku, *Petyos* atveju, tai tiems visiems *ransomwarams* jiems gerą vardą sugadino, nes jie deklaruodavo, kad jie visą laiką dešifruoja, tai jiems yra labai svarbu – jie teikia paslaugą, nes čia kaip paslauga yra." (E6, asmeninis interviu, 2017 m. liepos 26 d.). E3 ekspertas kalbėdamas apie atsarginių kopijų darymą pažymėjo, jog atsarginės kopijos turėtų būti daromos ar nedaromos atsižvelgiant į saugomos informacijos svarbą: „Viskas priklauso nuo sistemos lankstumo. Atsarginės kopijos turi būt daromos, ar neturi, kiek yra svarbi informacija, kokios informacijos svarba. Mano patirtis parodo, kad tam tikroms sistemoms ir dalykams jos tiesiog nereikalingos. Pinigų išmetimas ir laiko. Kam saugot ko tau nereikia greičiau atstatyti? Tos atsarginės kopijos va būtent ir turi iškilti nuo specifikacijos. Ko tau reikia, ką sistema turi daryti, gal tau užtenka vieną kartą į DVD nurašei, kaip mus po 30 parų sunaikinam ir viso gero." (E3, asmeninis interviu, 2017 m. liepos 21 d.). E7 ekspertas kalbėdamas apie atsarginių kopijų darymą pažymėjo, kad būtinas atsistatymo iš atsarginių kopijų testavimas ir gerosios atsarginių kopijų darymo praktikos principų laikymasis, kuris bendrai reikalauja daug finansinių resursų: „Dažnai būna taip, kad atsargines kopijas darosi, bet išlupti jų niekas niekada nebandė, nes situacijos tokios nebuvo ir staiga reikia pabandyti, tai... Dar yra tas su atsarginėmis kopijomis, taisyklė 3-2-1: mažiausiai 3 kopijos dvejose vietose ir viena vieta turi būti nutolusi fiziškai. Na, iš tikrųjų tai aš sakyčiau, tai labai didelė prabanga daryti kažkur atsargines kopijas ir jas kažkur laikyti, tai tikrai nemaža prabanga. Nes ir pati duomenų saugojimo įranga ji naudojama tiktai tam ir ji nėra pigi." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Kalbėdami apie kitą pasyvią priemonę – *honey pots* ekspertai pateikė skirtingas nuomones, nuo ypač skeptiškų *honey pots* atžvilgiu, išsakytų E3 eksperto, kuris pažymėjo, kad *honey pots* yra nepakankamai efektyvi priemonė atsakyti į šių dienų kylančius iššūkius, kai kibernetinė priešprieša tarp atakuojančiųjų ir besiginančiųjų šalių evoliucionuoja nuo paprasto kibernetinio incidento sisteminių kibernetinių karinių veiksmų link, todėl atsiranda poreikis konceptualiai pakelti reagavimo veiksmus į kibernetinės gynybos (angl. *cyber defence*) lygmenį: „Vadinkime taip: tai yra atgyvena ir tie kas supranta, *honey potai* visi. Technologijos keičiasi ne dienomis, o valandomis. Jei tu tapai potencialiu taikiniu, tai tave išlauš bet kokiu atveju. Klausimas – ar tu pamatysi ir kada tu pamatysi? **Tai vat, visa va ta atsparumas, nuo atsparumo prasideda saugumas, t.y. aktyvios priemonės iki kibernetinės gynybos sąvokos, kurios niekas nenori *cyber defence* dar naudoti, arba nesupranta, nes tai realiai yra karas."** (E3,

asmeninis interviu, 2017 m. liepos 21 d.). E2 pažymėjo *honey pots* kaip techninių priemonių apribojimus ir išsakė nuomonę, kad tai nėra pati tinkamiausia priemonė kibernetiniam atsparumui didinti. Kalbėdamas apie kitas pasyvias priemones ekspertas akcentavo IPS ir IDS sistemų praktinę naudą: „Viena iš priemonių, tie *honey pots*, bet reikėtų įsivaizduoti, kad hakeriai dažniausiai jei jie į įmones (organizacijas) yra nusitaikę, jie turi taikinį, jie žino apie tokius dalykus, apie galimai naudojamas priemones, net ir *Wannacry* virusas, kuris prieš mėnesį paplito ir LT pažeidė daugelį sistemų, jis jau turėjo įrankį, kaip pasitikrinti ar jis veikia *sandboxe* [*mechanizmas atskirti veikiančias programas, dažniausiai siekiant apriboti sistemos pažeidimus ir sutrikimus nuo išplitimo – aut.*]), uždarose sistemose, ar jo laboratorijose netestuoja saugumo specialistai – jis nesiaktyvuodavo. Tos priemonės tikrai ne panacėja. Neakcentuočiau, jos nepadeda apsisaugoti, jos geresnę vizualizaciją arba suklaidinimą hakerių padeda padaryti, bet pasitikėti jomis neverta, nes jos nėra efektyvios. Su jomis pačio atsparumo nepadidinsi. Čia daugiau aš akcentuočiau į IDS'us ir IPS'us, jos suteikia tau matomumą ir aliarmo galimybę nuo atakų ankstyvosios stadijos, jei pas tave anomalija tinkle, jei tipinės atakos, įsilaužimai, tokios sistemos padeda identifikuoti, tokius veiksmus ir generuoti aliarmą, t.y. įspėjimą administratoriui, kad čia vyksta kažkas negero ir taip galima proaktyviai sureaguoti į tokias [*anomalijas, atakas – aut.*]. Tos sistemos nėra pigios, jos kainuoja, bet yra ištisa pramonė, kuri kuria IDS'us, IPS'us, tai vat jų naudojimas yra racionalesnis, nei naudoti *honey pots.*" (E2, asmeninis interviu, 2017 m. liepos 14 d.). E4 ekspertas išsakė nuomonę, kad *honey pots* galėtų nukreipti įsilaužėlių dėmesį, bet tokia priemonė nebūtų veiksminga prieš motyvuotus įsilaužėlius: „Čia tokia kaip dėmesio nukreipimo priemonė. Vėlgi prieš rimtus žaidėjus tai tik laikina priemonė." (E4, asmeninis interviu, 2017 m. liepos 24 d.). E5 ekspertas akcentavo investicijų į visas reagavimo priemones svarbą, eksperto manymu, tam turėtų būti vykdoma atakų ir grėsmių analizė: „Reikėtų vertinti investiciją ir jos grąžą. Vėl būtų įdomu analitikų įžvalgos kokią dalį tų atakų sudaro neaukštos kvalifikacijos ir kokią dalį jau tikslingos atakos, parengtos ir tokios intelektualios." (E5, asmeninis interviu, 2017 m. liepos 24 d.). E1 ekspertas akcentavo *honey pots* naudą, tačiau pažymėjo, kad tokio pobūdžio sistemas būtina taikyti atsakingai: „Nusikaltėlio veikimą tu matai, kokiais metodais jis bando įsilaužti, o tu gali tvarkytis savo. Iš kitos pusės, reikia pamatuoti, kad nebūtų, kad tu žiūri kaip jis veikia, o tu norėdamas sustabdyti veikimą realioje sistemoje, pradedi kažką modifikuoti atverdamas skylę kažkur kitur, ir jis tą žinodamas specialiai provokuoja tai padaryti. Reik pasverti visus jų veiksmus, kad nebūtų kažkokių... Tiesiog ir yra testai ir visą kitą, kas yra labai svarbu reguliariai atlikti." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). E7 eksperto manymu, jei *honey pots* galėtų padidinti sistemos saugumo būklę nors 2–3 proc., ir kartu dar padėtų suklaidinti įsilaužėlius – tai gali būti naudotinu, visą bendrą kibernetinio saugumo sistemą papildančiu komponentu: „Jeigu tai padidina saugumą nors ir 2–3 proc., tai reiškiasi, kad tai jau yra naudinga. Kadangi jeigu tu gali ten padaryti mažiau saugumo, kad jis lengviau įsilaužtų ir ten laikyti *feikinius* [netikrus – *aut.*] duomenis ar dar kažką negu savo tinkle. Tokiu metu, kai jis laužiasi ir tu dar stebi tinklą ir pamatai, kad laužiasi, tai tu turi daugiau galimybių apsisaugoti savo tikrąją infrastruktūrą ir aš manau, kad tai nepasenęs dalykas ir jis turėtų būti. Jeigu leidžia finansai." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Apibenrinti reakcijos į atakas gerinimo faktoriai pateikiami 19 paveiksle.



Šaltinis: *parengta autoriaus*

19 pav. *Reakcijos į atakas gerinimas – ontologinė schema*

Reakcijų į atakas gerinimas yra viena daugiausiai faktorių apimančių kategorijų. Didžiausia dalis ją sudarančių faktorių yra vadybiniai faktoriai. 19 paveiksle geltona spalva išskirtas adekvačių atakoms priemonių formavimo faktorius yra būdingas visoms trims kategorijoms. Nes adekvačios priemonės gali apimti žinojimo ir technologinius elementus. Kalbant apie technines priemones ekspertai ypač akcentavo tinkamą atsarginių kopijų darymo valdymą. Šis elementas skirtinas ir vadybiniuose reakcijos į atakas gerinimo elementuose, juo akcentuojamas atsistatymo iš atsarginių kopijų procesų procedūrinis tobulinimas.

3.7. Atakos paviršiaus mažinimas siekiant padidinti kibernetinį atsparumą

Įvertinus, kad globaliu bei individualios organizacijos mastu atakos paviršius nuolatos didėja, tai ypač jaučiama atsirandant tokiems reiškiniams kaip daiktų internetas, BYOD.

Šią sritį apima tokios priemonės kaip darbuotojų mokymai apie žinomas atakas, socialinę inžineriją, organizacijoje naudojamos programinės įrangos skaičiaus mažinimas, visos kitos įmanomos priemonės. Ryšio prieigos taškų mažinimas, sistemos sudėtingumo mažinimas, nereikalingų komunikacijos kanalų mažinimas. BYOD modelis, kuomet darbuotojai atsineša savo darbo priemones: nešiojamus bei planšetinius kompiuterius arba naudoja darbinę kompiuterinę įrangą asmeninėms reikmėms. Tačiau privačiame sektoriuje tai jau tapo pakankamai plačiai paplitusia praktika. Pagrindinė motyvacija taikyti šį modelį – darbuotojai yra pripratę su savo planšetiniu kompiuteriu namuose dirbti, tad nereikia nuolatos keisti savo darbo įpročių, kaitalioti įrangos. Dėl to niveliuojamos ribos tarp kompiuteryje saugomų asmeninių ir organizacijos elektroninių duomenų. Taip pat blanksta ir apsaugoti būtinų objektų ribos. Esant situacijoms, kai konkretaus darbuotojo planšetinis kompiuteris yra nesaugus, šia priemone darbuotojas jungiasi prie darbinės sistemos, kelia grėsmę šiai sistemai ir visai su ja susijusiai infrastruktūrai. Valstybinėse organizacijose Lietuvoje nėra taikomas, tačiau jis gan populiarus privačiame sektoriuje, o tokiuose valstybėse kaip Jungtinė Karalystė, kuri 2013 m. priėmė BYOD taikymo viešojo sektoriaus organizacijose reglamentuojančius teisės aktus, sudarė sąlygas plačiam šio modelio naudojimui[33].

Esminiai organizacijos atakos paviršiaus mažinimo faktoriai. Kalbėdamas apie bendras atakos paviršiaus didėjimo tendencijas bei organizacijose pastaruoju metu intensyviai augančių prieigos mechanizmų skaičių E4 ekspertas pastebėjo, kad atakos paviršiaus mažinimas tampa ypač sudėtingu uždaviniu: „Dar nelabai senu laiku, viskas buvo paprasta ir aišku, kai buvo principas minimalumo. Naudoti tik tai kas būtina, viską ko nereikia išjungti ir neturėti galvos skausmo, o dabar su ta via įvairove, prieigos mechanizmų, kai atsiveriam viskam, tas principas tarsi sunkiai įgyvendinamas.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.). E3 ekspertas nemato atakos paviršiaus mažinimo per prieigos taškų ribojimą, eksperto nuomone, būtina procedūrinėmis priemonėmis įgyvendinti principą, kad „viskas yra draudžiama kas neparašyta, kad galima“: „Mano supratimu, atakos, vadinkim taip, jautrių taškų per kuriuos gali patekti mažinimas yra netgi nesvarstytinas. Jo tiesiog nebus. Kam gaišti laiką ir galvoti kaip tau sumažinti IP adresų kai gyvenimas pats privers, viskas atsiverinės, tu esi pasiruošęs apžioti vis didesnį arbūzą ir taip bus, todėl reikia galvoti kaip tiek techninėmis priemonėmis, tiek procedūrinėmis apriboti žmonių laisves ir įgyvendinti principą: viskas yra draudžiama kas yra neparašyta kad galima. O ne taip kaip yra dabar: viskas yra galima, kas neparašyta, kad draudžiama. Kol tas principas neveiks, tol visi mes turėsime bėdų. Jis tiesiogiai koreliuojasi su kibernetinio saugumo raštingumu, jeigu žmogus taip supranta, kad: ‚taip, tas yra negerai, na tada klausimų ir nekyla, mažinimo aš nematau‘. Reik susigalvoti, susiplanuoti savo technines priemones, kad tu bent jau techninėm priemonėm galėtum apriboti šituos dalykus. Ir aišku procedūros, kurios viską draudžia ir leidžia tik tai kas yra.“ (E3, asmeninis interviu, 2017 m. liepos 21 d.). Kalbėdamas apie BYOD populiarumo tendencijas bei asmeninių įrenginių naudojimą darbo tikslams E5 ekspertas pažymėjo, kad tai turėtų būti vengtinas dalykas, taip pat tai liečia asmeninių reikalų tvarkymą darbiniuose kompiuteriuose: „Dedikuoti įrenginiai turėtų būti, net jei

33 https://www.gov.uk/government/collections/end-user-devices-security-guidance http://www.computerweekly.com/news/2240206170/Government-approves-BYOD-for-public-sector-staff

leidžiama asmeninius naudoti, tai mano manymu, saugos reikalavimus turėtų nustatyti organizacija asmeniniams naudojamiems įrenginiams. Taip pat, kad būtų reikalavimas, jog tas įrenginys būtų dedikuotas tarnybai. Reiškia neturėtų jame būti asmeninės informacijos nesusijusios su darbu ir atvirkščiai – asmeniniame neturėtų būti darbinės. Reiškia dedikuoti įrenginiai, jei nėra galimybės skirti tarnybinius įrenginius. Tų asmeninių įrenginių sprendimą, turbūt labiau verslas galėtų taikyti. Kita vertus, ir draudimų retokai pasitaiko. Reiškia turbūt gana įprasta, kad asmeniniai įrenginiai vis tik panaudojami. Arba dokumentai tvarkomi asmeniniuose, persiunčiami į savo paštą." (E5, asmeninis interviu, 2017 m. liepos 24 d.). E4 ekspertas pažymėjo, kad BYOD valstybės tarnyboje principai plačiai nėra taikomi, tad jei kažkas nutartų juos pritaikyti praktikoje, tai būtų pritaikančiojo problema. Kitas klausimas, kurį išskyrė E4 ekspertas tai jungimasis prie darbinių sistemų iš asmeninių kompiuterių, esančių darbuotojų namuose, t.y. darbas iš namų. Pasak eksperto, niekas negali garantuoti galinio įrenginio saugumo: „Jei jau leidi tokius dalykus, įsivertink rizikas, kurias tai kelia. Jei jos tave tenkina – puiku, bet tai leisti viską ir skųstis, kad pas tave nesaugu, tai čia yra skųstis ant savęs paties. Pats sukėlei problemą, pats ją spręsk. Čia sudėtinga, bet galbūt įmanoma. Pvz., aš negirdėjau, kad pas mus VT leidžiama dirbti su savo atsineštais kompiuteriais. Negirdėjau tokių atvejų, po senovei, tai yra, jei kažkas leidžiama į asmeninį kompiuterį, tai yra kontroliuojama, tokios neesminės paslaugos. Ar čia vieša paslaptis, kad administratoriai dirba iš namų. Nors ir VPN'us turi, bet koks ten galinis įrenginys ir kas ten yra dar tai..." (E4, asmeninis interviu, 2017 m. liepos 24 d.). Tačiau E4 eksperto manymu, vien draudimai šioje situacijoje nebūtų veiksminga priemonė, kadangi dažnai darbu iš namų padidinamas darbuotojų lankstumas ir operatyvumas, todėl reikėtų ieškoti kompromisų: „Bandydamas sukontroliuoti konfliktuosi su savo darbuotojais, vienas dalykas, kita, tai gal jie negalės taip efektyviai dirbti. Taip, jis gali reaguoti bet kuriuo paros metu, praktiškai jei kažkas įvyksta. Tai toks naudos ir kaštų balansas pastoviai." (E4, asmeninis interviu, 2017 m. liepos 24 d.). E1 ekspertas akcentavo būtinybę sudaryti programinės įrangos juoduosius ir baltuosius sąrašus: „Turi būti įmonėse parengti juodieji/baltieji įrangos sąrašai. Turi būti paprasti vartotojai neturėtų admino teisių turi būti atskirtos naudotojų ir adminų paskyros. Jau mažinamas vektorius, kad praradus naudotojo paskyrą būtų maksimaliai maža žala. Dokumentaliai tas yra sutvarkyta, bet kaip tas praktikoje ar įmonės turi *active directory*, kur centralizuotai valdo, vartotojus, valdo politikas, ar neturi. Jei turi uždarą sistemą, nuo visko atsiriboja, bet neturi pašto administratoriaus ir perka cloudo [*debesų kompiuterijos – aut.*] paslaugą, *cloude* visą laiko susirašinėjimą, kam tada saugoti visą perimetrą jei pats atiduodi savo noru informaciją, kur pašte ne ką mažiau konfidencialios informacijos. Jei tokios informacijos nėra, paėmus visą visumą ten galima surinkti daug jautrios informacijos. Dėl to ir yra, kad pasisverti reikia smarkiai šitoje vietoje. Netgi kai kurių perteklinių įrankių naudojimas gali duoti tau žalą – iš to gero noro ir verslui trukdai ir pats spragą padarai." (E1, asmeninis interviu, 2017 m. liepos 11 d.). E7 ekspertas pateikė panašius siūlymus, eksperto nuomone, reikėtų viską griežtai reglamentuoti, o kalbant apie apribojimus, vertėtų uždrausti prieigą net prie asmeninio pašto paskyrų: „Reglamentavimas, netgi iki tokio, kuris yra, pavyzdžiui, KAM sistemoje. Yra programinė įranga tam tikra, kuri yra leista diegti. Ji patikrinta, ten, sakykim, naršyklė *Internet Explorer*, ten *Winzip* ar dar kažkas, *Offisas* ir jokių papildomų programinių įrangų būt

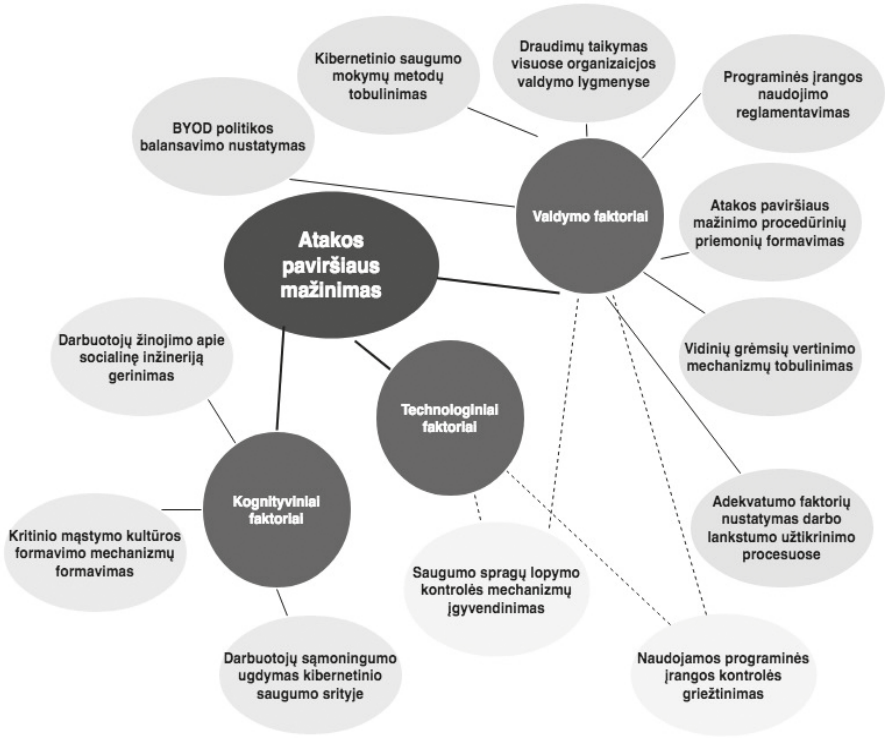
negali. Netgi yra padaryta taip, kad tam tikri failai exe, jie net nepasileidžia. Tai pirmasis metodas sumažinti va tą pažeidžiamumą, tai uždrausti vartotojams patiems būti administratoriais ir diegti kažką, fizinis ribojimas laikmenų nešiojimo ir taip toliau. Interneto naudojimas tarnybiniuose kompiuteriuose ribojamas. Kad tu negalėtum užeiti į tą patį elektroninį paštą, į tą viešą asmeninį gmailą. Jis tiesiog uždraustas, prie jo neprisijungia. Jeigu tau reik į *eBay*, tai tu neturėtum savo darbo laiku to daryt, eik namo arba pasiimk savo telefoną ir užeik iš jo. Kam kelti grėsmę? Tai vat vartotojų teisių ribojimas. Kai tu vartotojui duodi mažiau veiklos darbiniame kompiuteryje, tuo tu labiau apsaugai save. Ir administratoriams irgi, taisyklės yra vienodos visiems. Ir taisyklės turi galioti ir vadovui, ir pavaldiniui, o ne taip, kad vadovui viskas galima, jis vos ne torrentus norėtų siųstis į darbinį, o paprastam darbuotojui net į paštą negalima pažiūrėti." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). E6 manymu, sprendimas leisti ar ne darbuotojams naudotis darbui savo asmeniniais kompiuteriais, turi būti priimamas atsižvelgiant įmonės profilį, tačiau su kritine infrastruktūra dirbančiose organizacijose tai turėtų būti griežtai draudžiama, nepaisant to, turi būti taikomos papildomos saugos priemonės: „Nuo įmonės priklauso, ką ten ta įmonė, jei kažkokia kavos parduotuvė... Nuo įmonės specifikos, nuo užimamų pareigų, tas BYOD, ypač jei tu dirbi su kažkokioms kritinėms infrastruktūromis, tai turėtų būti draudžiama. Arba turėtų būti sertifikuoti, užtikrinti tai, kad paėmus telefoną ar kažką nenuimtų tu, nes yra paštas, duomenys. *Laptopuose* dar daugiau ten informacijos, tik kask. O jei priėmi tą sprendimą, kad tu nešiojiesi tą riziką, susigyveni tada ir turi būti tam tikros kontra priemonės. Tai šifravimas su kortele, biometriniai duomenys, dviejų faktorių autentifikacija, bet kas, aišku turi būti *hardas* [*kietasis diskas – aut.*] šifruotas." (E6, asmeninis interviu, 2017 m. liepos 26 d.). Kalbant bendrai apie atakos paviršiaus mažinimą, visi diskusijoje dalyvavę ekspertai sutiko, kad iš šios perspektyvos pažeidžiamiausia grandis yra žmogus, ypač ryškiai šiuos teiginius iliustravo E5 eksperto pateikti socialinės inžinerijos atakų praktiniai pavyzdžiai: „Labai svarbus ir gan pažeidžiamas, ir gan silpnas elementas yra žmogus. Valstybės tarnyboj ir bendrai bet kurioje organizacijoje, visokie socialinės inžinerijos atakos, kur bandoma išvilioti informaciją, tiesiog gyvai, telefonu. Labai efektyvios, deja..." (E5, asmeninis interviu, 2017 m. liepos 24 d.). Šios organizacinės grandies silpnumas pasireiškia įvairiomis formomis pradedant tuo, kad darbuotojai atidarinėja neaiškaus turinio nuorodas reklaminiuose elektroniniuose laiškuose: „Pavyzdžiui, marketingas labai *muša* per tą saugumą, tiesiog pasiūlymai. Jie gražūs visi, nuorodos paslėptos HTML. Bet jei siųstu jas tekstu, tai realiai matytų ir nuorodą. Vartotojas matytų, kad čia tikrai ne bankas, o kažkas kitokio. O kai pakiša po HTML'u jis paprasčiausiai nemato. Visi paveiksliukai, neaišku iš kur jie *loadinami*. Marketingas į tai žiūri, kad tai yra patrauklu vartotojui, o iš saugumo pusės..." (E6, asmeninis interviu, 2017 m. liepos 26 d.); patiki melagingais laiškais iš bankų: „Atrodo taip įprasta, lyg ir žino žmonės ir vis tiek pas mus pasitaiko va tokių užsikabinimų. Kad ir tuo elektroniniu paštu kada siunčiama Nežinomas siuntėjas, bet jei tai pranešimas neva iš banko, tai jis labai efektyviai veiks." (E5, asmeninis interviu, 2017 m. liepos 24 d.); patys darbuotojai instaliuoja nesaugią programinę įrangą: „VPN'ą uždraudė, pvz., bet neuždraudė darbuotojams pasileidinėti programų ir žmogus atsineša programos kilnojamą versiją, kuri pažeidžiama ir darbuotojas jungiasi per ją, nes nebuvo ugniasienės taisyklės parašytos, kad ją blokuoti. Jis varo per visą sieną SSL protokolu ir darykit jūs jam ką norit ir nieko

neapsaugosit. Bet viskas turbūt atsiremia į rizikų vertinimą ir grėsmių vertinimą, per kur tu gali būti pažeidžiamas. Nes jei tu neturi sistemų pasiekiamų iš išorės (svetainė, portalas, savitarna), tai kam tau reikalingas ten WAF'as [*ugniasienė – aut.*] ar dar kažkas." (E1, asmeninis interviu, 2017 m. liepos 11 d.). Kartais draudimai padeda sumažinti atakos vektorius, tačiau egzistuoja tendencija, kad darbuotojai jiems nuolatos ieško apėjimo kelių: „Tai viską apribojus, vektorių sumažina, bet vis tiek jis išlieka. Žmogus gi *Gmail*'ą atsidarys. Gali *Gmail*'o, *flash*'o neleisti, bet žmogus įsijungia Tor'ą [*Tor – programinė įranga įgalinanti anoniminę komunikaciją ir naršymą – aut.*], Tor'o reik neleisti. Tor'as iš esmės gali draust, bet *ransomwaro* atakom, tada pamatysi kas užvaldo kompiuterį, nes jie komunikaciją daro per Tor'ą ir tada matysi. Draudimas neįvyks kai komunikacija vyks, bet vis tiek turi stebėti, žmogus turi analizuoti tuos logus, kad matytų kas vyksta tinkle. Bet visi tie proxy gali pasidaryti. Tas draudimas neišeis, jei žmogus biški įgudęs." (E6, asmeninis interviu, 2017 m. liepos 26 d.). E5 ekspertas pastebėjo, kad tam tikrais atvejais vis dar suveiktų ir klasikinis kibernetinių nusikaltėlių metodas – virusais užkrėstų USB atmintinių platinimas organizacijoje ir jos prieigose, siekiant, kad jas radę darbuotojai iš smalsumo ar geranoriškumo jas patalpintų į savo kompiuterius ir taip užkrėstų sistemas virusais. Pagal E5 ekspertą, tokia situacija atskleidžia, kad vis dar trūkstamas elementas yra personalo atsparumas: „Taip, čia irgi klasika, bet manau, kad tikrai suveiktų, nes iš geriausių paskatų žmogus norėtų patikrinti kieno ir atiduoti. Dovanos, tie patys *flashiukai* ir įvairios IT dovanos labai populiarios. Šiuo metu kaip tik parengę esame ministerijos darbo reglamento pakeitimą, kur iš didesnės rizikos valstybių priėmus dovanas, nejungti į darbo vietas, nei į turimą nešiojamą kompiuterį komandiruotėje, nei grįžus, o pateikti mūsų departamentui įvertinimui ir tik konstatavus, kad yra saugu, jos bus grąžintos. **Tai vat tas vidinis atsparumas, atsparumas asmenų personalo darbuotojų prasme, reikėtų dar daug įdirbio**." (E5, asmeninis interviu, 2017 m. liepos 24 d.).

Pagrindinės organizacijos atakos paviršiaus mažinimo priemonės ir iššūkiai. Taisytina situacija gali būti įvairiomis priemonėmis, pradedant E6 eksperto akcentuojamu administratorių teisių valdymu: „Žinoma, kontrolė ir išvis niekas neturėtų administratoriaus teisių turėti išskyrus tuos, kas supranta ką daro. Bet atsirado virusai *ransomwarai*, kurie iššifruoja vartotojo teises. Kiekvienam atvejui atsiranda vis kitas, tokio lankstaus, kaip bambuko nepadarysi, nes gali padaryti maksimaliai saugią, arti to, bet tuomet ja naudotis bus neįmanoma, trikampį žinot tą: patogumas, saugumas, funkcionalumas?" (E6, asmeninis interviu, 2017 m. liepos 26 d.); baigiant darbuotojų mokymu, už kurį pasisakė dauguma ekspertų. E2 ekspertas šiuo klausimu pastebėjo, kad būtent švietimas yra ypač aktualus augant socialinės inžinerijos atakoms: „Darbuotojų mokymą akcentuočiau, nes dabar tendencijos iš šių dienų atakų yra labai išaugęs atakų vektorius – socialinė inžinerija. Panaudojant žmogiškuosius faktorius, žmogiškąsias silpnybes, išgaunant slaptažodžius įvairiais socialiniais metodais, skambinant sekretorei. Personalo mokymas kritinį mąstymą turėti dėl kibernetinio saugumo pavojų. Ir kritiškai reaguoti į visokius užklausimus. Pavyzdžiui dideli pinigai yra šiuo metu prarandami naudojant laiškus nuo direktoriaus neva buhalterei, prašant pervesti pinigus skubiai į užsienio sąskaitą užsienio partneriui. Ir tokie nepakankamai informuoti žmonės kaip buhalteriai, kurie nežino, kad gali būti tokie sukčiavimo kibernetiniai atvejai perveda pinigus ir tai dideli nuostoliai ir problemos didelės ir

čia su bankais, jie bando identifikuoti ir nurodyti, kad informuotumas ta linkme eina." (E2, asmeninis interviu, 2017 m. liepos 14 d.). E7 ekspertas taip pat akcentavo švietimo naudą, kuri yra viena iš pagrindinių priemonių atsižvelgiant į emocijomis besivadovaujančių žmonių prigimtį: „Tiktai švietimas vartotojų. Žmogus, jisai labiau reaguoja į emocijas, o visos tos soc inžinerijos, ant emocijų juk ir pastatyta korta. Tai vat, bet kaip tu žmogų bešviestum, kaip tu realiai jam rodytum visa tai, jis vis tiek reaguos į emocijas, netgi jei ir viską žino. Galbūt kai tu pats padarysi tokią socialinę inžineriją, o paskui darbuotojams parodysi rezultatus, kad aš va padariau ir jūs pažiūrėkite ant kiek mes esame pažeidžiami. Kitą kartą darbuotojas jau ims galvoti ar čia ne vėl kokie aferistai, ataka kažkokia. Galbūt netgi tokius – mokymas per pabandymą, per realią patirtį, o ne tik, kad: ‚imkit paskaitykit, imkit prezentaciją paklausykit', tas ne visada padeda..." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). E5 ekspertas taip pat akcentavo švietimo būtinybę, iliustruodamas socialinės inžinerijos praktiniais pavyzdžiais: „Tiktai švietimas. Sunku įsivaizduoti kas čia dar galėtų pagelbėti. Įvairiausių yra tų socialinės inžinerijos metodų ir jie visi efektyviai suveikia kaip bebūtų keista. Buvo RRT pratybos organizuojamos. Ir jie panaudojo ir socialinės inžinerijos metodą. Ir „skambutis iš Prezidentūros" praktiškai išgauna visą informaciją. Ir tas skambutis žmogui, kuris dirba su Prezidentūros IT padaliniu arba įslaptintų reikalų tvarkymų, tai tu gali atskirti, kad nėra tokio darbuotojo, nes tu tiesiog žinai tai. Nežinančiam pakanka pasakymo ir tokiu būdu išviliojama reikalinga informacija, kodai. Tai mes turėjom čia tokių problemų, atskirą pašnekesį turėjom apie socialinę inžineriją. **Apie darbuotojus kalbant: gynyba ir atsparumas dažnai yra sutelkiamas dėmesys į išorę ir mažesnis dėmesys skiriamas darbuotojams, t.y. atakai iš vidaus ir ji būna paprastesnė, nes nereikia lipti nei per langus, nei per duris veržtis, spynas rakinti.** O tiesiog tai padaroma, kad ir socialinės inžinerijos metodu iš vidaus. Tai vat šitas atsparumas dar toli gražu iki aukšto lygio." (E5, asmeninis interviu, 2017 m. liepos 24 d.). E6 ekspertas ypač akcentavo švietimą, eksperto manymu, būtent švietimas aktualus visose kibernetinio saugumo veiklose: „Švietimas tai 100 procentų aišku. Čia ant viso švietimas. Nes kiber higienos jei nėra, tai viskas... Toliau aišku priklauso kokie resursai turi būti." (E6, asmeninis interviu, 2017 m. liepos 26 d.). Kalbėdami apie techninės apsaugos priemones, ekspertai jas mato po švietimo principų įtvirtinimo bei kritinio mąstymo kultūros, ir išskiria IDS ir IPS sprendimus bei savalaikius programinės įrangos tiekėjų pateikiamus saugumo spragų taisymus: „Techniniai įrankiai, po švietimo, po to kritinio mąstymo jau naudoti įrankius tuos IDS'us, IPS'us, dar naudoti svarbiau yra sistemų spragų lopymą [angl. *patching*], pažeidžiamumų mažinimui, ar per penetration testus, ar tiesiog gamintojas rūpinasi savo programinės įrangos saugumu ir skyles lopo, bet dažna problema yra, kad tų atnaujinimų [*saugumo – aut.*] nėra įdiegiama, nors va gamintojas *Microsoft* yra pristatęs atnaujinimus kovo mėn. [*interviu vykdytas liepos mėn. – aut.*], bet mes saugumiečiai buvome nustebę kiek daug sistemų Lietuvoje ir pasaulyje „neužpačintų", kurias minėtas *Wannacry* virusas ir pažeidė." (E2, asmeninis interviu, 2017 m. liepos 14 d.). Atsižvelgiant į diskusijos pokrypį dalis ekspertų buvo paklausti ar veiksminga būtų stiprinti programinės įrangos tiekėjų kontrolę, bandant suintensyvinti saugumo spragų išleidimus. E2 ekspertas pažymėjo, kad programinės įrangos gamintojai jau dabar dirba pakankamai stresinėmis sąlygomis ir nemažai nuveikia stiprindami savo produktų saugumą, skirdami finansinius paskatinimus spragas

suradusiems programuotojams ir kitais mechanizmais: „Apie tai buvo kalbama prieš 5–7 metus, dabar jau nematome poreikio tiekėjų spausti, kad jie saugumo spragas lopytų, nes tų saugumo spragų tiek atrandama ir tiek jos išnaudojamos, kad jau yra tiems tiekėjams klausimas išlikimo versle. Kad jie išliktų, jie turi tą daryti ir jie tą daro maksimaliai, kiek pajėgia ir dar labiau juos spausti jau nėra tokio poreikio, sakyčiau. Jie turi komandas, netgi nėra viešai šnekama, yra mokama taip vadinamiems baltakepuriams, tiems baltiesiems *hackeriams*, daro įvairius konkursus, tu atrandi pažeidžiamumą: 'tu neparduok jo juodojoje rinkoje tiems blogiečiams *hackeriams*, ateik pas mus į *Microsoft*, mes tau sumokėsim, kad radai pažeidžiamumą mūsų programose'. Ir tas veikia, ir daug yra organizacijų, kurios iš to uždirba, bet ji nenuteka organizuotam nusikalstamumui. Todėl kas mėnesį ir dažniau *Microsoftas* „patchina" savo *Windows* operacines sistemas, mes gaunam „patchus" ir juos įdieginėjame užtai, kad tokia industrija veikia." (E2, asmeninis interviu, 2017 m. liepos 14 d.). Kaip alternatyva tiekėjų programinei įrangai galėtų būti pačioje organizacijoje sukurti programiniai sprendimai, tačiau eksperto teigimu, vertėtų pasitikėti gamintojais ir kol jie dar neišleidžia programinės įrangos saugumo spragų atitaisymų, pačiai organizacijai būtina proaktyviai imtis saugos priemonių: „Iš senų laikų mūsų visos sistemos yra padarytos „in the house" [*organizacijoje – aut.*]. Bet sprendimai yra gamintojų, tu aišku visada turi pasitikėti, nes jei gamintoju tu nepasitiki, tai nežinai kokį ir „patchą" gausi. Kitas dar yra variantas, ką organizacijos daro – dar net jei nėra atnaujinimo, tai jie uždeda ant *firewall*'o ar IDS'o kažkokias taisykles, kur paprasčiausiai tas pažeidžiamumas nebus išnaudotas. Ir lauki atnaujinimo. Tai va tie saugumo žmonės tikrai turi daug to darbo, nes reikia konfigūruoti ir portus ir IDS'us, ir IPS'us, ir *firewall*'us. Pavyzdžiui, domenus užblokuoti visus, kurie yra tarkim *porno*. Na, kur organizacijose neisi, palikti tuos dažniausius." (E6, asmeninis interviu, 2017 m. liepos 26 d.). Apibendrinti organizacijos atakos paviršiaus mažinimo faktoriai pateikiami 20 paveiksle.



Šaltinis: *parengta autoriaus*

20 pav. *Atakos paviršiaus mažinimas – ontologinė schema*

Pažymėtina, kad nepaisant to, kad didžiausią atakos paviršius plotą organizacijoje sudaro technologijos, apklausti ekspertai visuotinai pripažino, kad pažeidžiamiausias elementas šioje situacijoje yra – žmogus. Tad ši atsparumo didinimo kategorija praktiškai neturi techninių elementų – jai priskirtini du, kurie 19 paveiksle pažymėti geltona spalva. Iš dalies, tai apima technologines priemones, tačiau visa šių elementų esmė yra tinkamas reglamentavimas, kuris vėliau įgyvendinamas techninėmis priemonėmis. Pažymėtina, kad ekspertai ypatingai akcentavo visus tris kognityvinius faktorius, t.y. žinojimą apie socialinę inžineriją, kritinio mąstymo formavimą ir sąmoningumo ugdymą kibernetinio saugumo srityje. Plačiausiai aptartas valdymo faktorius yra BYOD politikos nustatymas.

3.8. Rizikų valdymo gerinimas siekiant padidinti kibernetinį atsparumą

Rizikų valdymas literatūroje laikomas vienu iš esminių atsparumo aspektų. Dažnai manoma, jog atsparumas beveik tiesiogiai susijęs su rizikų valdymu – kaip organizacija sėkmingai valdo rizikas, tiek ji yra atspari. Taigi šioje tyrimo dalyje buvo bandoma nustatyti,

kaip būtų galima tobulinti rizikų valdymą tipinėje valstybinėje organizacijoje Lietuvoje: gerinant rizikų valdymo, vertinimo mechanizmus, tobulinant pasirengimo procesus įvairiais lygmenimis: operacinių rizikų, taktinių, strateginių rizikų?

Rizikų valdymo svarba organizacijos kibernetinio atsparumo didinimui. Kalbėdami apie rizikų valdymo ypatumus Lietuvos viešojo sektoriaus organizacijose kai kurie tyrimo dalyviai buvo ganėtinai skeptiški: „Didelis klausimas – ar valstybinėse, ar daro tą rizikų valdymą? Yra tokia VRM'o knygutė išleista – „Rizikų valdymo vadovas". Kaip vienas sakė žmogus: ‚Imkit tą vadovą, paskaitykit ir jūs viską suprasit.' Tada labai gerai supratau, kad tas žmogus net nebuvo jo atsivertęs, kad jeigu jis siūlo paskaityti tą vadovą, kad suprasti visas rizikas." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). Didžioji dalis ekspertų akcentavo, kad rizikų valdymas bendrame kibernetinio saugumo kontekste yra svarbus procesas, tai yra bazinis, pamatinis faktorius plėtojant kibernetinio saugumo veiklas organizacijoje: „Jei žiūrėti bendrai, rizikų vertinimas yra visko pamatas. Nuo jo turi viskas prasidėti vienareikšmiškai. Tu turi įsivertinti informaciją ir kaip grėsmės atsiranda, per kur tu tą informaciją gali prarasti ir kaip informacija gali būti paveikta, rizikas įsivertini, kas su tuo gali būti, iš principo tada pasirenki tu rizikų mažinimo priemones ir tu dirbi, žaidi su tuo." (E1, asmeninis interviu, 2017 m. liepos 11 d.); „Rizikų valdymas jau dabar priimtas ne tik standartuose, ISO 27 serijos standartai, kur tu, jeigu nori įdiegti saugumo standartus, tai rizikų valdymas yra pamatinis dalykas. Nuo to viskas ir pradedama. Bet dabar jeigu net ne standartus diegi, įprasta ir siūloma daryti rizikos analizes tam, kad identifikuoti savo silpnąsias vietas ir jomis užsiimti [...] labai reikalingas dalykas." (E2, asmeninis interviu, 2017 m. liepos 14 d.). E4 eksperto manymu, organizacijoje rizikų visumos valdymas yra vienas iš pagrindinių uždavinių, nepaisant to, kokio pobūdžio rizikos tai bebūtų. Tačiau dažnai organizacijoje yra pamirštama, kad IT rizikos yra bendra visų rizikų dalis, tad jos valdymas turi būti integruotas į visų kitų organizacijai kylančių rizikų visumą. Tik aukštą rizikų valdymo kultūrą turinti organizacija geba apimti visas rizikas, jų nediversifikuodama: „Na, visų pirma, tai reikėtų pasakyti, kad vienas iš pagrindinių organizacijos uždavinių, bet kokios. Čia kalbant apskritai: veiklos rizika, finansinės, teisinės, trečiųjų šalių. Rizikos yra visuma ir visos tos IT rizikos ir kibernetinės yra dalis bendros [*rizikų dalies – aut.*]. Bet apie tai yra dažnai užmirštama, tiksliau ta vat bendroji dalis eina savaime suprantama, o vat IT yra specialistų darbas ir sąsajų tarp tų dviejų dalykų nėra. Nors iš tikrųjų visoms rizikoms valdyti reikalingi ištekliai, o darant taip atskiriant dirbtinai. Tai yra pamirštama, kad tai yra visuma ir turėtų būti valdoma kaip visuma. O šiaip tai, jeigu daugiau gilinantis, jeigu rizikos valdymo kultūra organizacijoje yra gera, tai ji suvaldys ir IT rizikas visas." (E4, asmeninis interviu, 2017 m. liepos 24 d.). E1 eksperto nuomone, yra kritiškai svarbu nuolatos vertinti paskutinę informaciją ir remiantis ja atnaujinti rizikos vertinimus, šio proceso rezultatas turi būti aiškus visiems organizacijos nariams: „Atsiranda nauja grėsmė, atsiranda naujos informacijos, vėl tu vertini rizikas, žiūri, tau tai svarbu, nesvarbu, todėl ta rizikų vertinimo metodika, vieninga visai VT, gal nepritempsi, bet gairės, principai, kriterijais, kuriais tą rizikų vertinimą turi atlikti. Kad suprastų visi turbūt gal irgi nepavyks, bet kažkaip supaprastinti, kad ir kiekvienam būtų aišku kaip ką kur reikia pasidaryti, ką kur žinoti, ką kur atkreipti dėmesį ir nuo ko pradėti ką daryti." (E1, asmeninis interviu, 2017 m. liepos

11 d.). Ypač tai svarbu atsižvelgiant į tendenciją, kad atsiranda atvejų, kai su į IT sritimi susijusias problemas kitos organizacijos dalys įsiklausyti nenori, padėtį galėtų pagerinti nebent kultūros ir požiūrio kaita: „Yra viena negera tendencija, t.y. *aš nieko apie tai nežinau*. Vat turim kažką, padalinį IT, kuris viskuo pasirūpinti. Kultūrą turbūt, nuo supratimo kažkokio reikėtų pradėt." (E4, asmeninis interviu, 2017 m. liepos 24 d.). Nors galutiniam vartotojui tai gali ir nebūti kritinis faktorius, organizacijos mastu tai yra procesas, kurį būtina plėtoti ir daryti tai reikėtų organizacijos vertikale iš viršaus žemyn: „Jeigu apie rizikų valdymą naivu šnekėti paprastiems *end-useriams* [*galutiniams vartotojams – aut.*], bet įmonei(organizacijai) rizikos valdymas ir tas pats verslo tęstinumo planas yra labai naudingas dalykas, na, beveik dalykas – *must* [*būtinas – aut.*], sakyčiau." (E2, asmeninis interviu, 2017 m. liepos 14 d.). E1 eksperto manymu, rizikų valdymas kaip atskaitos taškas dar svarbus ir tuo, kad darant jį iki sistemos diegimo veiksmų, galima įvertinti IT sistemoms reikalingas investicijas: „Nuo rizikų turi prasidėti, nes tu tuomet žinosi kiek reik tau investuoti, tu žinosi kokia informacija yra kritinė, kur gali patirti didžiausią žalą. Sako, kad rizikos vertinimą turi daryti saugos vadovas, IT, ne jie turi daryti - verslas turi. Sauga, IT gali *pasuportinti* [*palaikyti – aut.*], bet verslas turi pasakyti. Nes *adminui* yra nesvarbu, ar „Jonas Jonaitis" šita info yra svarbi ar ne. Jam tai yra bitų laukas, kuris yra tam tikroj DB, o kiek tas yra svarbu turi atsakyti verslas. Bet tas irgi turi būti pakankamai pasverta, kad nebūtų užkelta vertė tam tikriems dalykams ir didinamas atsparumas ar saugumas ne to ko reikia. Dėl to vat ir yra tas saugos vadovo, saugos įgaliotinio, konsultanto buvimas kaip patariamasis – ar jums tas yra tikrai svarbu, jei tą prarasit, jums net šitas nebesvarbu." (E1, asmeninis interviu, 2017 m. liepos 11 d.). E6 ekspertas pastebėjo, kad pakankamai svarbu laikytis rizikos valdymą apibrėžiančiuose sertifikatuose nustatytų principų ir vykdyti valdomos informacijos kategorizavimą pagal darbuotojų kompetenciją: „Viskas tvarkoj su tais rizikų vertinimais, ISO standartais. Jie padeda, jei jų laikaisi, jei jų nesilaikai, tai net nereikia sertifikuotis. Ten viskas yra aprašyta, žmogiškieji resursai, įrangos resursai, kaip valdoma, kaip informacija klasifikuojama konkrečiai. Pavyzdžiui, Snowdeno atveju, jis informacijos negalėjo paimti, tai vat čia informacijos klasifikavimo vienas iš dalykų, kad tu negali vienas žmogus turėti prieigos prie visos informacijos, tai čia tas iš rizikų ir yra, bet tą patį sako ir ISO standartas, tas 2007, kad negali būti informacija vienoje vietoje, turi būti diversifikuota, išskaidyta." (E6, asmeninis interviu, 2017 m. liepos 26 d.). E1 ekspertas kalbėdamas apie rizikų valdymo srities sertifikatus pažymėjo, kad viena pagrindinių jų sukuriamų verčių yra ta, kad galima įvertinti situaciją iš šalies: „ISO sertifikacija yra kuo gerai, kad atsiranda išorės auditoriai, kurie iš šono pasižiūri. O būtent valstybės institucijos nelabai skiria pinigų, jie daro vidinius auditus, valstybės kontrolės, bet valstybės kontrolė jie nežiūri tiek giliai, nes jų mastas yra kitoks. Dėl to kažkas turėtų institucijose 1 kartą per 2–3 metus pasižiūrėti iš šalies." (E1, asmeninis interviu, 2017 m. liepos 11 d.). Taip pat E1 ekspertas akcentavo ir informacijos kategorizavimo svarbą: „Dėl to ir reik kategorizavimo sistemos. Jei tavo IS dirba su tokiais duomenimis, tu turi atitikti tokius reikalavimus, jei tu imi duomenis iš tokios sistemos, tu turi irgi atitikti tokius reikalavimus. Kad to būtų laikomasi ne tik teoriniame, bet ir praktiniame lygmenyje ir atvirkščiai – praktika turi sutapti su dokumentais. Dirbant VRM tekdavo žiūrėti nuostatus IS ir tu atsiverti dokumentą, o jis lygiai toks pats, kaip kitos insttucijos, kur tu jau žiūrėjai ir patvirtinai. Bet tu turi pats

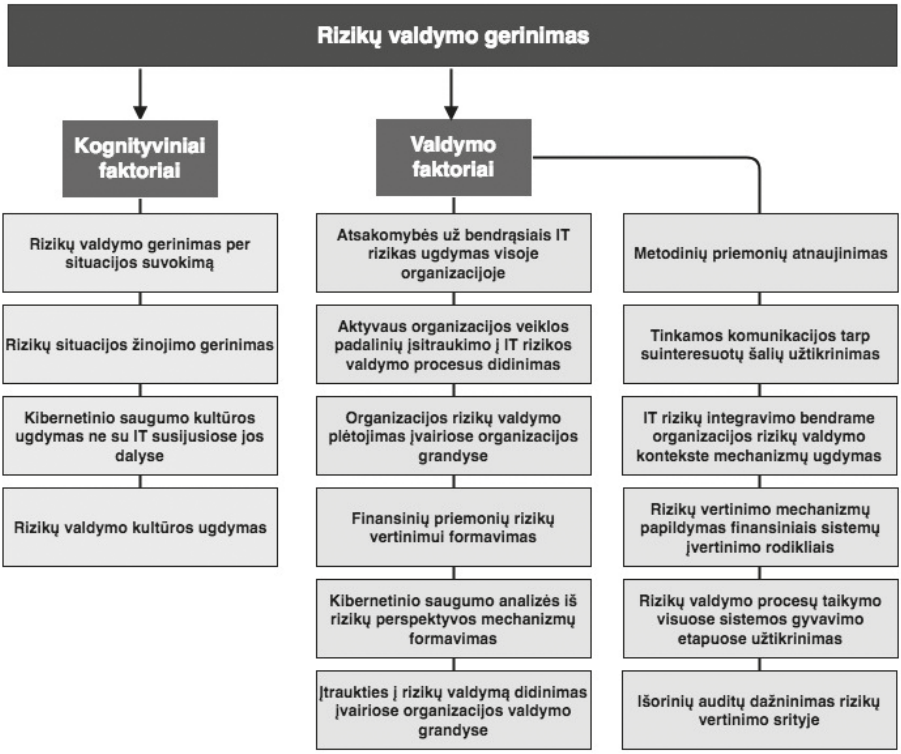
[nuostatų rengėjas – *aut.*] įsivertinti, ar tu tikrai taip darysi kaip yra dokumente, jei tu darysi *backupą* kas 1 valandą, nes tau svarbu duomenų praradimas, tu sukiši tokius pinigus, o realiai tau nėra tai reikalinga. Arba parašai, kad darysi kas 1 valandą, o darai 1 kartą į savaitę... Dėl to tas turi būti svertas protingumo, jei nusirašinėji, nusirašyk protingai, žiūrėk pagal save. Daug VT institucijų, kur parašo lyg turėtų 4 atskirus duomenų centrus, o realiai stovi serveris po stalu." (E1, asmeninis interviu, 2017 m. liepos 11 d.).

Rizikų valdymas – dabartinė būklė. Su ekspertais diskutuota ir apie tai, kaip reikėtų gerinti esamus rizikų valdymo procesus. Kaip pažymėjo E3 ekspertas, remdamasis atsparumo diagrama, rizikų valdymas turėtų egzistuoti sistemos palaikymo ir jos gyvavimo procesuose iki jos kritimo ir būtent tinkamas rizikos valdymas padėtų sugrįžti jai į pradinę būseną. Kad jį užtikrinti būtina užtikrinti tinkamą komunikaciją tarp proceso dalyvių: „Rizikų valdymas yra tiesiogiai susiję su kompanijos, organizacijos, aljanso narių, skirtingų padalinių gebėjimo bendradarbiauti ir keistis informacija, t.y. informacijos sklaida ir viešinimas apie procesus, darbus, įrangą ir t.t. Jeigu to darbo nėra, tai tada automatiškai žmonės nesupranta pavojų, jei nesupranta pavojų, tai negali sugalvoti riziką, kuri galėtų atsirasti jo sistemose, tuomet kai kitas padalinys kažką darys. Kuo daugiau personalas žinos, kas vyksta, kokios sistemos dalyvauja ir, kaip jos tarpusavyje susiję, tuo bus geresnis rizikos valdymas." (E3, asmeninis interviu, 2017 m. liepos 21 d.). E5 ekspertas pažymėjo, kad nors pats rizikų procesas ir neblogai reglamentuotas, metodines priemones atnaujinti reikėtų, kasmetiniai atliekami rizikų vertinimai ganėtinai formalūs, o į bendrą rizikų procesą turėtų įsitraukti daugiau organizacijos atstovų, ne tik saugos įgaliotiniai. Apie platesnį organizacijos įsitraukimą į rizikų valdymo procesus kalbėjo ir E7 ekspertas, kuris pažymi, kad po truputį tas įsitraukimo mastas auga dėl didėjančio vadovų suvokimo ir aiškumo, jog tai neįmanoma padaryti vienam asmeniui ar organizaciniam junginiui: „Tai vėlgi rizikų valdymo vienintelis dalykas – įtraukti kuo daugiau žmonių į tą rizikos valdymo procesą ir įtraukti visus, iš visų tų sektorių, sakykime, įmones. Ir nuo valdžios atstovų ir specialistų ir paprastų vartotojų ir administratorių, nepalikti tų rizikų valdymo vien tik IT departamentui ar IT personalui. Dabar tiesiog ateina supratimas tas labiau iš valdžios, valdžia jau labiau supranta. Atsiranda kibernetinė kultūra. Galbūt atsiranda pas pačius vadovus, nes kasdien apie tai girdi, kasdien mato. Visokie kibernetiniai nusikaltimai, kibernetiniai įsibrovimai ir t.t. Pradeda apie tai mąstyti ir gal jei vertina rizikas kažkokias, bando visus įtraukti, turbūt visi supranta, kad vienam žmogui neįmanoma to padaryti. Reikalingas sisteminis požiūris į viską ir įtraukimas įmonės organizacijos. Čia manau ne tik valstybiniam tinka, bet ir verslui. Paskui kai atsiranda suvokimas, tuomet ir atsiranda noras kažką daryti ir taip toliau." (E7, asmeninis interviu, 2017 m. rugpjūčio 14 d.). E1 ekspertas taip pat pažymį VRM išleisto „Rizikų valdymo vadovo" atnaujinimo poreikį: „Dabar yra ten ta rizikų valdymo metodika VRM'o 2004–2006 m. parengta – šablonas, bet kaip bebūtų jau 11 metų praėjo." (E1, asmeninis interviu, 2017 m. liepos 11 d.). Kalbėdamas apie išorinių auditų dažnio didinimą, E4 ekspertas įvertino tokį pasiūlymą gan skeptiškai, motyvuodamas tuo, kad auditoriui nepakaktų laiko tinkamai į ją įsigilinti: „Nežinau, ar dažninimas padėtų, bet auditas tai įprastinė tokia kontrolės priemonė, jis laikas nuo laiko daromas. Pas tave nuolatos sėdės auditorius. Ne tai, kad trukdys darbą, tiesiog pas tave situacija keičiasi ne taip greitai, kad jis kažką rastų. Tai manau, kad čia irgi toks balanso dalykas kas kiek tai daroma. Kas

man rodos daromas išorinis auditas. Na, dar valstybės kontrolė, tai čia atskirai, tai yra būtina priemonė.“ (E4, asmeninis interviu, 2017 m. liepos 24 d.). Nepaisant to, egzistuojanti geroji praktika rodo, kad reikėtų pritarti E5 eksperto teiginiui dėl išorinių rizikos vertinimų: „Jei valdytojas yra protingas, viskas tvarkoj, jeigu labai formaliai žiūrėtume tai būtų labai sunku pagrįsti. Tiek atitikties, tiek rizikos vertinimo išorinis aspektas labai svarbus objektyvumo prasme, visai kito požiūrio prasme negu viduj organizacijos.“ (E5, asmeninis interviu, 2017 m. liepos 24 d.). Paklaustas, ar veiksminga priemonė būtų sudarinėti rizikų sąrašus, E3 ekspertas pastebėjo, kad rizikų valdymas turėtų būti organizuojamas remiantis akcentuojant ne pačias rizikas, o vykdomų veiklų rizikas: „Rizikų valdymas su rizikų sąrašu čia galbūt truputi ne taip turėtų būti. Ne rizikų sąrašas, bet veiksmų rizika. Tai tu turi prieš darydamas kažkurį veiksmą, tu turi įsivertinti riziką. O tam tu turi rizikos vertinimo tam tikros praktikos, kuriose užpildžius tam tikrą dokumentaciją rizikos vertinimo metu, tu pamatai, kad va tam turės įtakos ir tam. Ir tuomet per dokumentacijos pildymą tu gali įsivertinti kaip tu tą riziką mažinsi ir ją valdysi. Tau reik gamintojo atstovo, ar tau užtenka savų žmonių. Tau reikia papildomų leidimų, pavyzdžiui, formalumų, ministerijos ir t.t. Taigi yra rizikos vertinimo formalumas, kai tu turi įsivertinti kiekvieną savo būsimą veiksmą planuojamą. Kai jau vyksta griuvimas, tada jau popieriai nepildomi. Tada jau vyksta reagavimas, pagal tam tikrą nustatytą tvarką ir aišku atsižvelgiant į visas prieš tai buvusius rizikos vertinimus.“ (E3, asmeninis interviu, 2017 m. liepos 21 d.). Tokiu būdu, rizikos valdymas organizacijoje formuojamas iš vidaus į išorę. E1 ekspertas plėtodamas diskusiją apie egzistuojančias metodines priemones pažymi, kad galbūt jos nėra visiems rizikų vertinimams tinkama priemonė, taip yra dėl skirtingų požiūrių į tam tikrų rizikas keliančių aspektų vertinimą: „Gal kai kurie principai ten buvo, bet ten jis metodinis dokumentas ir ne visai tinkantis, nes vienos įmonės vertinasi poveikį gyvybei, poveikį finansams, pasireiškimo mastą, tarkim tris šiuos aspektus. Kiti vertina du ir vertina poveikį gyvybei ir sveikatai ir tikimybę pasireiškimą. Ir jis rašo, kad pas jį rizikos yra mažos, o kodėl mažos, dėl to, kad jo sistemos duomenys niekaip neįtakoja gyvybės ir sveikatos, tai vadinasi – blogai parengta dedamoji, jis turi vertinti ne gyvybę, o kažką kitą arba šalia gyvybės dar kažką kitą. VT vertinant iš praradimo informacijos rizika gyvybei tai yra ligoninių sistemos ir turbūt policijos FNTT, STT, kur gali būti liudininkai dar kažkas, kad jei tą informacija skleidi, žinai, ką pašalinti, kad tau byla būtų nutraukta, nes nebėra liudininkų. Mes daug kur akcentuojam, kad yra poveikis gyvybei, bet kaip bebūtų, su VT sistemoms to poveikio nėra. Vat su elektros, dujų, vandens tiekimu, ten yra poveikis gyvybei. Taip, tos pačios grėsmės yra tas grėsmių sąrašas, vokiečių 46 grėsmės, berods, pradedant gaisru, vandens, atakos, vagystės, jie ne veltui jį sugalvojo.“ (E1, asmeninis interviu, 2017 m. liepos 11 d.). Iš proaktyvesnių priemonių E6 akcentavo auditavimo poreikį, siekiant įvertinti atsparumą konkretaus pobūdžio atakoms, išskyrė galimybes daryti imituotas atakas bei, kalbėdamas apie technines priemones, pasiūlė prevenciškai išskirti su padidintos rizikos aplinkomis dirbančius įmonės padalinius į atskirus potinklius, taip izoliuojant juos nuo kitų organizacijos dalių: „Auditavimas, dar galim daryti tas imituotas atakas, ypač *spearphishing*'*o*, *CEO frauď o* ar *frauď o*, tas paprastas, kur nėra sudėtinga vieną kartą per mėnesį. Aišku dar ir žmonės, kurie dirba su kažkokia rinka, gauna *emailus*, *attachmentus*. Išsiaiškinus visą struktūrą fizinę įmonės, galima juos į atskirą potinklį išskirti. Jei kažkas įvyktų, tai jie

savo tam smėlio dėžėje. Taip, gali atskirti tam tikrus sektorius, departamentus išskaidyti. Ir ten kiekvienam IDS'ą statyti. Kaip ir sakau – tinklo architektūra yra labai svarbi. Pirma. išsiaiškini ką įmonė daro, už ką skyrius atsakingas. Jei ten tik vienas paštu bendrauja – kažkokios vienos priemonės gali būt. Ten kiti, tarkim, bendrauja su rytų rinka, na tai rytų rinka tarkim didesnis rizikos faktorius pagal dabar geopolitinę situaciją, tai dar kitaip, bet čia kiekvienu atveju reik analizuoti pačią tą įmonę ir tada spręsti." (E6, asmeninis interviu, 2017 m. liepos 26 d.).

Apibenrinti kibernetiniių rizikų valdymo gerinimo faktoriai pateikiami 21 paveiksle.



Šaltinis: *parengta autoriaus*

21 pav. *Rizikų valdymo gerinimas – ontologinė schema*

Kaip matoma 21 paveiksle, ši kategorija neturi nei vieno technologinio faktoriaus, o didžiausią jos dalį sudaro vadybiniai faktoriai. Nagrinėjant kognotyvinius faktorius vertėtų išskirti IT saugumo kultūros ugdymą ir bendrą rizikų kultūros ugdymą organizacijoje. Šie du faktoriai turi glaudžią sąsają su dviem vadybiniais: veiklos padalinių įsitraukimu į IT rizikos procesus ir organizacijos rizikos valdymo plėtojimas įvairiuose organizacijos grandyse.

3.9. Kibernetinio atsparumo principų formalizavimas kibernetinio saugumo teisės aktuose Lietuvoje: tyrimo rezultatai

Lietuvos Respublikos kibernetinio saugumo įstatymas. Kaip pažymima Valstybės kontrolės (2015) atliktame kibernetinio saugumo audite, Lietuvos Respublikos kibernetinio saugumo įstatymas (toliau – Kibernetinio saugumo įstatymas) priimtas bandant užpildyti egzistuojančias kibernetinio saugumo srities valdysenos spragas, t.y. nustatyti kibernetinio saugumo srities politiką formuojančias ir įgyvendinančias institucijas, kibernetinio saugumo srities valdymo ir kontrolės principus, dalyvių pareigas bei atsakomybes. Vertinant Kibernetinio saugumo įstatymą iš atsparumo perspektyvos, naudojant PEF, Linkov, NIST kibernetinio atsparumo matricą, galima išskirti kelias atsparumo principus apimančias sąsajas. Ryškiausias Kibernetinio saugumo įstatymo ryšys su PEF, Linkov, NIST atsparumo matricos Planavimo-pasirengimo dalies Informacine, Socialine ir Kognityvine dimensijomis ir Adaptavimosi dalies Informacine dimensija. Sąsajos matomos nagrinėjant Kibernetinio saugumo įstatyme deklaruojamas kibernetinio saugumo sistemos dalyvių funkcijas, pagal kurias, Vyriausybė: „2) tvirtina Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką ir ypatingos svarbos informacinę infrastruktūrą ir (arba) šios infrastruktūros valdytojų sąrašą; 3) tvirtina organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus ypatingos svarbos informacinei infrastruktūrai, organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus valstybės informaciniams ištekliams“; Krašto apsaugos ministerija: „1) rengia ir teikia Vyriausybei tvirtinti organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus ypatingos svarbos informacinei infrastruktūrai, ir organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus valstybės informaciniams ištekliams“; VRM: „rengia ir teikia Vyriausybei tvirtinti Ypatingos svarbos informacinės frastruktūros identifikavimo metodiką ir ypatingos svarbos informacinę infrastruktūrą ir (arba) šios infrastruktūros valdytojų sąrašą“. Šie Kibernetinio saugumo įstatymo punktai atitinka PEF, Linkov, NIST matricos informacinės dalies 1, 4, 5 uždavinius, apibrėžtus Planavimo-pasirengimo dimensijoje, kuri išskiria: fizinės-aparatinės įrangos ir priemonių, sistemų, programinių platformų inventorizaciją, vertybių kategorizavimą pagal jų jautrumą ar atsparumo reikalavimus, bei kritinės aparatinės ir programinės įrangos teikėjų kvalifikaciją. LKSĮ apibrėžtas Vyriausybės atsakomybes taip pat apima incidentų bei ypatingos infrastruktūros incidentų valdymo planų tvirtinimą: „4) tvirtina Nacionalinį kibernetinių incidentų valdymo planą; 5) tvirtina tipinius kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus“. Krašto apsaugos ministerija savo ruožtu: „2) rengia ir teikia Vyriausybei tvirtinti Nacionalinį kibernetinių incidentų valdymo planą; 3) teikia Vyriausybei tvirtinti tipinius kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus; 4) tvirtina ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus“. Šios dvi Vyriausybei ir keturios KAM deleguojamos užduotys atitinka PEF, Linkov, NIST matricos Planavimo-pasirengimo dalies Kognityvinės dimensijos pirmąjį uždavinį, apimantį Sistemos būsenos ir įvykių numatymą. Nacionalinio kibernetinio saugumo centro, kuriam pagal kompetenciją yra skirta ypatingos svarbos informacinių infrastruktūrų kibernetinių incidentų valdymo padalinio veikla, atitinka minėtą PEF, Linkov, NIST matricos punktą,

vykdant Kibernetinio saugumo įstatyme numatytas užduotis, apimančias trečiąjį ir septintąjį punktus: tipinių kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planų rengimą bei ypatingos svarbos informacinių infrastruktūrų kibernetinių gynybos planų rengimą. Kibernetinio saugumo tarybai pagal Kibernetinio saugumo įstatymą priskiriamos funkcijos, būdingos PEF, Linkov, NIST matricos Socialinės dimensijos Planavimo-pasirengimo ir Adaptacijos dalims. Pagal Kibernetinio saugumo įstatymą, KST: „1) teikia pasiūlymus kibernetinio saugumo dalyviams dėl kibernetinio saugumo prioritetų, plėtros krypčių, siektinų rezultatų ir jų įgyvendinimo būdų; 2) teikia pasiūlymus kibernetinio saugumo dalyviams dėl platesnio viešojo sektoriaus, verslo ir mokslo bendradarbiavimo galimybių kibernetinio saugumo užtikrinimo srityje; 3) analizuoja kibernetinio saugumo užtikrinimo tobulinimo tendencijas, teikia kibernetinio saugumo dalyviams išvadas ir pasiūlymus dėl kibernetinių incidentų valdymo; 4) teikia kibernetinio saugumo dalyviams rekomendacijas dėl kibernetinio saugumo stiprinimo“. PEF, Linkov, NIST matricos Socialinės dimensijos Planavimo-pasirengimo dalies pirmąjį uždavinį apima išorinių subjektų, kuriems gali kilti kibernetinė grėsmė, identifikavimą ir šeštąjį uždavinį, susijusį su kibernetinio saugumo žinojimo kultūros formavimu. Taip pat tai glaudžiai sietina su Socialinės dimensijos adaptacijos dalies trečiuoju ir ketvirtuoju punktais, apimančiais informacijos apie paskutines grėsmes valdymą bei esamos padėties žinojimą, informacijos dalijimąsi su išorinėmis suinteresuotomis šalimis. Pagal Kibernetinio saugumo įstatymą NKSC užduotys apima visų PEF, Linkov, NIST matricos dimensijų Planavimo – pasirengimo dalį, taigi nagrinėjant NKSC priskiriamas veiklas, identifikuotinos tam tikros sąsajos su PEF, Linkov, NIST matricos fizinės dimensijos detektavimo dalies pirmuoju uždaviniu – siekiant nustatyti potencialius kibernetinio saugumo įvykius vykdyti fizinės aplinkos stebėseną (PEF). Pagal Kibernetinio saugumo įstatymą, NKSC „atlieka valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams stebėseną“. NKSC numatytas vaidmuo – „teikti konsultacijas ir rekomendacijas valstybės informacinių išteklių valdytojams ir ypatingos svarbos infrastruktūros valdytojams kibernetinio saugumo klausimais; vykdo informacijos sklaidą kibernetinio saugumo klausimais“. Šis NKSC vaidmuo priskirtinas PEF, Linkov, NIST matricos Socialinės dimensijos Planavimo-pasirengimo dimensijos šeštajam punktui „Kibernetinės kultūros formavimas“ bei Socialinės dimensijos trečiajam uždaviniui „Būti informuotam apie paskutinius pavojus bei vėliausias apsaugos tendencijas, dalintis šia informacija organizacijoje ir ketvirtajam uždaviniui „Savarankišku informacijos dalinimusi su išorinėmis suinteresuotomis šalimis, siekiant platesnio kibernetinio saugumo situacijos žinojimo“. Taip pat identifikuotinos Kibernetinio saugumo įstatymo sąsajos su PEF, Linkov, NIST matricos Kognityvinės dimensijos Detektavimo dalies pirmuoju uždaviniu, kuris numato „Detektuotinų įvykių analizę, siekiant suprasti atakų taikinius ir metodus“. LKSĮ ši veikla apibrėžiama NKSC uždaviniu, pagal kurį centras „analizuoja nacionalinę kibernetinio saugumo situaciją ir rengia nacionalinio kibernetinio saugumo būklės ataskaitas“. Reikia iskirti LKSĮ esantį NKSC veiklos punktą, kuris tiesiogiai apima kibernetinio atsparumo būklės įvertinimą. Pagal jį, NKSC turi teisę „**taikyti technines priemones, siekdamas įvertinti valstybės informacinių išteklių ir ypatingos svarbos informacinių infrastruktūrų atsparumą kibernetiniams incidentams“.** Nagrinėjant Kibernetinio saugumo įstatymą iš

bendrinės kibernetinio saugumo kultūros formavimo ir kibernetinio saugumo situacijos žinojimo perspektyvų, vertėtų išskirti Kibernetinio saugumo įstatyme numatytas užduotis visoms kibernetinio saugumo sistemoje dalyvaujančioms institucijoms – kibernetinio saugumo informacijos žinojimo gerinimą ir sklaidą. Šiems procesams įgyvendinti įstatyme numatytos NKSC pareigos: „Skelbti visuomenei kibernetinio saugumo užtikrinimo metodinę informaciją, rekomendacijas ir kitą su kibernetinio saugumo užtikrinimu susijusią neįslaptintą informaciją". Pagal Kibernetinio saugumo įstatymą, Asmens duomenų inspekcija „teikia visuomenei ir suinteresuotoms institucijoms informaciją apie kibernetinio saugumo, susijusio su asmens duomenų apsauga, rizikos veiksnius, pavojus ir grėsmes kibernetinėje erdvėje". Įstatyme numatyta, kad prie kibernetinio saugumo situacijos žinojimo turėtų prisidėti ir viešųjų paslaugų teikėjai, kurių pareiga yra „Viešai skelbti paslaugų gavėjams rekomendacijas apie priemones kibernetiniam saugumui užtikrinti naudojantis viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų teikiamomis paslaugomis". Kibernetinio saugumo rekomendacijų skelbimas yra ir elektroninės informacijos prieglobos paslaugų teikėjų pareiga. Ją vykdydami paslaugų teikėjai privalo „viešai skelbti elektroninės informacijos prieglobos paslaugų gavėjams rekomendacijas apie priemones kibernetiniam saugumui užtikrinti naudojantis elektroninės informacijos prieglobos paslaugomis". Reikėtų išskirti ir tarpinstitucinį bendradarbiavimą tiriant kibernetinius incidentus: „Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Policijos departamentas ir kitos policijos įstaigos bendradarbiauja tiriant kibernetinius incidentus, keičiasi su kibernetinių incidentų tyrimais susijusia informacija, reikalinga institucijų pagal kompetenciją vykdomoms funkcijoms atlikti. Prireikus apie kibernetinių incidentų tyrimą gali būti informuojami kiti kriminalinės žvalgybos subjektai ir (arba) žvalgybos institucijos". Pagal Kibernetinio saugumo įstatymą, numatytas NKSC bendradarbiavimas su individualiais asmenimis: „Pasitelkti į pagalbą informacinių technologijų ir kibernetinio saugumo specialistus; bei mokslo ir verslo organizacijomis: „kartu su verslo subjektais, mokslo ir studijų institucijomis ir kitais kibernetinio saugumo dalyviais plėtoti bendrus kibernetinio saugumo projektus".

Kalbant apie proporcingumo principo taikymo įtvirtinimą teisinio reguliavimo priemonėmis, pažymėtina, kad šis principas deklaruojamas ir Lietuvos Respublikos kibernetinio saugumo įstatymo trečiojo straipsnio antrame punkte: „Kibernetinio saugumo proporcingumo – taikomos kibernetinio saugumo užtikrinimo priemonės negali būti griežtesnės, negu būtina kibernetiniam saugumui užtikrinti, o taikomi teisiniai, organizaciniai ir techniniai kibernetinio saugumo reikalavimai neturi apriboti kibernetinio saugumo dalyvių veiklos kibernetinėje erdvėje labiau, negu tai būtina" (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

Apibenrinta Lietuvos Respublikos kibernetinio saugumo įstatymo analizė pateikiama 22 paveiksle.

	Planavimas / pasirengimas	Detektavimas	Absorbavimas	Atsistatymas	Adaptacija
Fizinė	0,5	1	0,5	0,5	0,5
Informacinė	1	0	0	0	1
Kognityvinė	1	0,5	0	0	0
Socialinė	1	0,5	0	0	1

Šaltinis: *parengta autoriaus*

22 pav. *Atsparumo principų perkėlimas į LR teisės aktus - Lietuvos Respublikos kibernetinio saugumo įstatymas*

Kaip matoma paveiksle, labiausiai Lietuvos Respublikos kibernetinio saugumo įstatyme apimamos Informacinės, Kognityvinės ir Socialinės dimensijų Planavimo-pasirengimo fazė, taip pat Fizinės dimensijos Deteketavimo fazė ir Informacinės bei Socialinės dimensijų Adaptacijos fazė. Tačiau beveik visiškai nėra sąsajų su visų dimensijų Absorbavimo ir Atsistatymo bei Detektavimo fazėmis. Darytina išvada, kad įvertinus Lietuvos Respublikos kibernetinio saugumo įstatymą naudojant PEF, Linkov, NIST atsparumo matricą, nustatyta, kad Lietuvos Respublikos kibernetinio saugumo įstatyme reglamentuojama tik dalis kibernetinio atsparumo komponentų.

Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. Be vienų pagrindinių Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo (toliau – LR informacinių išteklių valdymo įstatymas) tikslų – užtikrinti tinkamą valstybės informacinių išteklių kūrimą, tvarkymą, valdymą, naudojimą, priežiūrą, sąveiką, planavimą ir finansavimą, LR informacinių išteklių valdymo įstatymo paskirtis – el. informacijos saugos reglamentavimas. Įstatymas ne tik apibrėžia valstybės informacinių išteklių rūšis bei išteklių politikos formavimą, bet ir nustato tokių valdymo funkcijas atliekančių subjektų kaip Valstybės informacinių išteklių valdymo tarybos ir duomenų valdymo įgaliotinių veiklą, o kalbant apie techninių informacinių technologijų priemonių, kuriomis apdorojama institucijos valdoma informacija, saugą – ir valdymo ir saugos vertinimą (Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011). Kalbant apie LR informacinių išteklių valdymo įstatyme nustatomas institucijų funkcijas iš kibernetinio atsparumo perspektyvos, akcentuotinos VRM deleguojamos funkcijos, kurias vykdydama institucija „konsultuoja valstybės informacinių sistemų ir registrų valdytojus, valstybės informacinių sistemų ir registrų tvarkytojus, kitas institucijas valstybės informacinių išteklių saugos klausimais; nustato informacijos svarbos įvertinimo, valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo pagal jose apdorojamos informacijos svarbą kriterijus ir jų priskyrimo atitinkamai kategorijai tvarką“. Šios funkcijos sietinos su PEF, Linkov, NIST kibernetinio atsparumo matricos Socialinės dimensijos planavimo-pasirengimo šeštuoju uždaviniu „Kibernetinio saugumo žinojimo kultūros formavimu“. Taip pat Informacinės dimensijos Planavimo-pasirengimo ketvirtuoju uždaviniu, apimančiu „Vertybių ir paslaugų alegorizavimą, remiantis informacijos jautrumo reikalavimais“. Šias priemones atitinka ir LR informacinių išteklių valdymo įstatyme Valstybės informacinių išteklių valdymo tarybai deleguotos funkcijos, pagal dalį kurių institucija rengia pasiūlymus

ir rekomendacijas Vyriausybei dėl valstybės informacinių išteklių valdysenos ir „saugos reikalavimų, saugos dokumentų turinio gairių, informacijos svarbos įvertinimo, valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo pagal jose apdorojamos informacijos svarbą kriterijus ir jų priskyrimo atitinkamai kategorijai tvarkos".

Daugiau tiesioginių sąsajų su PEF, Linkov, NIST atsparumo matricoje apibūdinamomis dimensijomis identifikuoti yra sudėtinga, o tolimesnis LR informacinių išteklių valdymo įstatymo nagrinėjimas galimas nebent iš bendrinių atsparumo perspektyvų.

23 paveiksle pateikiama apibenrinta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo analizė.

	Planavimas / pasirengimas	Detektavimas	Absorbavimas	Atsistatymas	Adaptacija
Fizinė	0	0,5	0	0	0
Informacinė	1	0,5	0	0	0,5
Kognityvinė	0,5	0	0	0	0
Socialinė	1	0	0	0	0

Šaltinis: *parengta autoriaus*

23 pav. *Atsparumo principų perkėlimas į LR teisės aktus – Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas*

Kaip matoma paveiksle, labiausiai Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme apimamos Informacinės, Socialinės dimensijų Planavimo-pasirengimo fazė. Tačiau visiškai nėra sąsajų su visų dimensijų Absorbavimo ir Atsistatymo, Adaptacijos bei Detektavimo fazėmis. Darytina išvada, kad įvertinus Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymą naudojant PEF, Linkov, NIST atsparumo matricą, nustatyta, kad Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme reglamentuojama tik dalis kibernetinio atsparumo komponentų.

El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programa. El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programoje (toliau – El. informacijos saugos programa), remiantis skirtingomis saugos dalimis, išreikštomis skaitine išraiška ir apimančiomis reikalavimus: el. informacijos saugumui, incidentų šalinimui ir gyventojų kibernetinio saugumo pojūčiams stiprinti, nustatytas strateginis tikslas – „Plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 procentus visų valstybės informacinių išteklių, vidutinis ypatingos svarbos informacinės infrastruktūros incidentų likvidavimo laikas sumažėtų iki 0,5 valandos, o Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis pasiektų 60 procentų". Šiame tiksle įžvelgtinas bandymas formuoti kažką panašaus į kibernetinio saugumo kultūrą Lietuvoje, taip pat bendros saugumo būklės gerinimą ir reakcijos į atakas procesus per incidentų likvidavimo laiko trumpinimą. Atskirai vertėtų pažymėti, kad VK 2015 m. atlikusi El. informacijos saugos programos analizę pastebėjo, kad: „El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programa, kurioje planuota pasiekti daugiausia

rezultatų šioje srityje, vykdoma nerezultatyviai (bendras programos tikslų įgyvendinimas 2015 m. rugsėjo mėn. siekia 21 proc.)“. Nustatyti ne visi su kibernetinio saugumo ir el. informacijos sauga susijusių planavimo dokumentų tarpusavio ryšiai, vėluojama įgyvendinti planavimo dokumentuose numatytas priemones (VK, 2015). Nagrinėjant El. informacijos saugos programą iš atsparumo perspektyvos, pažymima, jog programos penktajame punkte deklaruojama, kad: „Programa atitinka Europos Komisijos 2009 m. kovo 30 d. komunikate KOM (2009) 149 „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – **geresnė parengtis, didesnis saugumas ir atsparumas** išdėstytas veiklos kryptis”.

El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos priedas. Kalbant apie El. informacijos saugos programos priede nurodytus konkrečius jai įgyvendinti numatytus tikslus, skirtini keli su atsparumo formavimu sąsajas turintys, šių tikslų įgyvendinimo uždaviniai ir jų įgyvendinimo vertinimo kriterijai. El. informacijos saugos programoje pirmuoju numeriu keliamas bendrinis saugumo užtikrinimo tikslas: „Pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas“. Jam įgyvendinti numatyta aibė uždavinių, kurių pirmasis (1.1.) – „Tobulinti elektroninės informacijos saugos (kibernetinio saugumo) koordinavimą ir priežiūrą“. Minėto uždavinio pasiekimo vertinimo kriterijaus (eilės Nr. 3) antroji dalis: „Įsteigta kolegiali nuolatinė elektroninės informacijos saugos (kibernetinio saugumo) konsultacinė taryba“. Šis vertinimo kriterijus sietinas su PEF, Linkov, NIST atsparumo matricos Socialinės dimensijos Planavimo-pasirengimo dalies šeštuoju punktu „Kibernetinės kultūros ugdymas“. Penktasis vertinimo kriterijus, nors ir nesietinas su matricos elementais, turi ryšį su literatūroje egzistuojančiais atsparumo gerinimo faktoriais per pažeidžiamumų valdymo gerinimą: „Patvirtintos grėsmių ir pažeidžiamumų vertinimo metodikos. Atliktų grėsmių ir pažeidžiamumų vertinimų skaičius Nevaldomų pažeidžiamumų dalis, procentais“ (eilės Nr. 5). Tikimasi, kad įgyvendinus El. informacijos saugos programos uždavinius 2019 m. tokių nevaldomų pažeidžiamumų liks tik 10 procentų nuo bendrojo pažeidžiamumų skaičiaus. Kitas šio uždavinio punktas „Elektroninės informacijos saugos (kibernetinio saugumo) atitikties reikalavimams stebėsenos sistema stebimų informacinių sistemų dalis, procentais“ (eilės Nr. 5) sietinas su PEF, Linkov, NIST atsparumo matricos Fizinės dimensijos Detektavimo dalies pirmuoju punktu „Fizinės aplinkos stebėsena, siekiant detektuoti potencialius kibernetinius įvykius“. El. informacijos saugos programos 1.3. uždavinys „Plėsti ir tobulinti saugią valstybės informacinę infrastruktūrą“ yra labiau taikytinas bendriniams saugos principams užtikrinti, tačiau jo vertinimo kriterijus „Valstybės valdymo poreikiams užtikrinti naudojamų ryšių ir informacinių sistemų rezervinių pajėgumų ir pagrindinių pajėgumų santykis, procentais“ (eilės Nr. 19) atspindi vieną kertinių atsparumo idėjų – pasirengimą nenumatytiems atvejams ir turi sąsajų su PEF, Linkov, NIST atsparumo matricos Kognityvinės dimensijos Planavimo-pasirengimo dalies pirmuoju punktu „Sistemos būsenų ir įvykių numatymas ir planavimas“. El. informacijos saugos programos 1.5. uždavinys „Plėtoti tarptautinį bendradarbiavimą elektroninės informacijos saugos (kibernetinio saugumo) srityje sietinas su bendrosios atsparumo bendradarbiavimo kultūros ugdymu. Vertinimo kriterijai, šio uždavinio pasiekimų įvertinimui nustatyti uždaviniai apima kelis atsparumo aspektus: „Sričių (Europos Komisijos 2009 m. kovo 30 d. komunikate KOM

(2009) 149 nurodytų uždavinių sprendimo ramsčių), kuriose bendradarbiaujama tarptautiniu lygiu, skaičius“ (eilės Nr. 25); „Dalyvauta NATO, Europos Sąjungos ir Jungtinių Tautų Organizacijos renginiuose elektroninės informacijos saugos (kibernetinio saugumo) klausimais, į kuriuos buvo kviečiama, procentais“ (eilės Nr. 26); „Dalyvauta tarptautinėse kibernetinės gynybos pratybose, į kurias buvo kviečiama, procentais“ (eilės Nr. 28); „Pasirašytų bendradarbiavimo su kitų valstybių CERT centrais susitarimų skaičius“ (eilės Nr. 29); Pažymėtina, kad vertinimo kriterijuose minimame komunikate KOM (2009) 149 „Dėl ypatingos svarbos informacinės infrastruktūros apsaugos Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“ pažymima, kad: „Šiuo metu ypatingos svarbos informacinės infrastruktūros saugumo ir atsparumo klausimai daugiausiai sprendžiami nacionaliniu lygmeniu, beveik nekoordinuojant Europos mastu [...]“, taigi El. informacijos saugos programoje išdėstyti uždaviniai yra savalaikiai ir padiktuoti egzistuojančio poreikio. Kaip pažymima komunikate, ES lygmeniu kibernetinės pratybos ir modeliavimas – tai „pagrindiniai dalykai siekiant didesnio ypatingos svarbos informacijos infrastruktūros saugumo ir atsparumo, yra pradiniuose vystymosi etapuose“, tad iš atsparumo perspektyvos vertinant tokios iniciatyvos yra labai reikalingos, o jų poreikis akcentuojamas ekspertų ir sudaro Kognityvinės PEF, Linkov, NIST matricos Atsparumo dimensijos Planavimo-pasirengimo dalies trečiąjį punktą, teigiantį scenarijais pagrįstą kibernetinės karybos ir gynybos (angl. *wargaming*) vykdymą. El. informacijos saugos programos tikslą Nr. 2. „Užtikrinti ypatingos svarbos informacinės infrastruktūros efektyvų funkcionavimą“ galima būtų apibūdinti kaip bendrinę kibernetinio saugumo siekiamybę, tačiau nagrinėjant šio uždavinio pasiekimų vertinimo kriterijus pastebima, kad egzistuoja aibė jų sąsajų su atsparumo idėjomis įvairiuose lygmenyse, ypač akcentuotinas sistemos atsistatymo greitis: „Vidutinis ypatingos svarbos informacinės infrastruktūros objektų incidentų likvidavimo laikas, valandomis“ (eilės Nr. 30); galima išskirti ir vertinimo kriterijų: „Identifikuotų ypatingos svarbos informacinės infrastruktūros objektų dalis, procentais“ (eilės Nr. 32), kuris sietinas su PEF, Linkov, NIST atsparumo matricos Informacinės dimensijos Planavimo-pasirengimo dalies pirmuoju uždaviniu „Fizinės įrangos, sistemų, programinės įrangos platformų ir programinės įrangos inventorizacija“. Šis uždavinys ir tos pačios dimensijos trečiasis – „Išorinių sistemų katalogavimas“ – sietini su El. informacijos saugos programos uždavinių veiklos vertinimo kriterijumi „Ypatingos svarbos informacinės infrastruktūros objektų, kuriuose atlikta kritinių išteklių ir teikiamų paslaugų analizė ir veiklos sutrikdymo, sutrikus šių objektų informacinėms infrastruktūroms ar šiems objektams būtinoms išorės informacinėms infrastruktūroms, rizikos vertinimas, dalis, procentais“ (eilės Nr. 32); taip pat, vertinant iš atsparumo perspektyvos ypač akcentuotinas su ypatingos infrastruktūros atsparumu tiesiogiai susijęs vertinimo kriterijus **„Ypatingos svarbos informacinės infrastruktūros objektų, kuriuose atliktas atsparumo vertinimas, dalis, procentais“** (eilės Nr. 34). El. informacijos saugos programoje užsibrėžtas tikslas, kad 2019 m. toks vertinimas bus atliktas šimtui procentų ypatingos svarbos infrastruktūros objektų. Fizinės PEF, Linkov, NIST atsparumo matricos dimensijos Detektavimo dalies pirmasis uždavinys, nustatantis būtinybę „Stebėti fizinę infrastruktūrą, siekiant nustatyti potencialius kibernetinius įvykius“, sietinas su El. informacijos saugos programos veiklos vertinimo kriterijumi,

matuojančiu ypatingos svarbos infrastruktūros procentą Lietuvos kibernetinės erdvės perimetre: „Nuolat stebimų ypatingos svarbos Lietuvos elektroninių ryšių ir interneto tinklų infrastruktūros ir Lietuvos kibernetinės erdvės perimetro elementų skaičius nuo visų, procentais“ (eilės Nr. 35) tiesiogiai nesietinas su jokia PEF, Linkov, NIST Atsparumo matricos dimensija, tačiau bendradarbiavimo perspektyvoje ir geros praktikos mainų kontekste svarbus Programos vertinimo kriterijus „Institucijų, dalyvaujančių Europos Sąjungos ypatingos svarbos infrastruktūros informacinio tinklo CIWIN (angl. *Critical Infrastructure Warning Information Network*) veikloje, skaičius“ (eilės Nr. 36). Taip pat aktualus vertinimo kriterijus „Paskirta institucija, atsakinga už ypatingos svarbos objektų veiklos tęstinumą informacinės infrastruktūros sutrikdymo metu“ (eilės Nr. 37). PEF, Linkov, NIST kibernetinio atsparumo Kognityvinės dimensijos Planavimo-pasirengimo dalies pirmais punktas sistemų įvykių ir būsenų planavimas sietinas su El. informacijos saugos programos vertinimo kriterijais „Patvirtintas valstybės gynybai skirtų institucijų ypatingos svarbos informacinės infrastruktūros objektų ir informacinių išteklių kibernetinės gynybos planas“ (eilės Nr. 38); „Patvirtintas nacionalinis ypatingos svarbos informacinės infrastruktūros objektų ir valstybės informacinių išteklių kibernetinės gynybos planas“ (eilės Nr. 34). Ypač svarbus ir ekspertų akcentuotinas iš atsparumo perspektyvos - alternatyvaus planavimo ir atsarginės infrastruktūros įgyvendinimas, kuris El. informacijos saugos programoje sietinas su vertinimo kriterijumi „Patvirtintas atsarginės infrastruktūros, reikalingos ypatingos svarbos informacinių infrastruktūrų gyvybiškumui užtikrinti, parengimo ir jos valdymo kritinių situacijų metu planas“ (eilės Nr. 39). Nagrinėjant trečiąjį programos tikslą „Užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje“ aibę šiam tikslui įgyvendinti formuojamų uždavinių, įžvelgtinos tiesioginės paralelės su tokiais atsparumo konceptais kaip kibernetinio saugumo situacijos žinojimo gerinimas, kibernetinio saugumo kultūros formavimas. Pirmuoju uždaviniu, deklaruojamu šioje programos tikslų dalyje, būtent ir nubrėžiama tokia siekiamybė: „3.1. kelti elektroninės informacijos saugos (kibernetinio saugumo) kultūrą“. Sėkmingu El. informacijos saugos programos įgyvendinimo atveju, šio uždavinio įgyvendinimo vertinimo kriterijuose išdėstyti pasiekimai turėtų gana glaudžias sąsajas su PEF, Linkov, NIST atsparumo matricoje Socialinėje Planavimo-pasirengimo dimensijose keliamais uždaviniais: šeštasis „Kibernetinės kultūros ugdymas, apimtų programos uždavinių vertinimo kriterijus“ – „Lietuvos gyventojų, suvokiančių kibernetinio saugumo principus, dalis, procentais (eilės Nr. 42); „Veikiančių savišvietos saugos tematika interneto svetainių skaičius“ (eilės Nr. 45); „Svetainių naudingumą teigiamai įvertinusių lankytojų dalis, procentais“ (eilės Nr. 45); „Organizuotų renginių, skirtų elektroninės informacijos saugos (kibernetinio saugumo) svarbos suvokimui gerinti, skaičius, vienetais“ (eilės Nr. 46); „Pranešimų spaudai apie elektroninės informacijos saugos iniciatyvas skaičius“ (eilės Nr. 48). Kalbant apie PEF, Linkov, NIST socialinės dimensijos adaptavimosi trečiąjį uždavinį „Informuotumas apie egzistuojančias grėsmių tendencijas, jų pasidalinimas su suinteresuotomis šalimis“, pažymėtina, kad šis uždavinys atitiktų El. informacijos saugos programos vertinimo kriterijus: „Parengtų elektroninės informacijos saugos (kibernetinio saugumo) specialistų rengimo ir jų kvalifikacijos tobulinimo programų skaičius, vienetais. Šias programas išklausiusių specialistų skaičius“ (eilės Nr. 43). Nagrinėjant trečiojo tikslo uždavinį 3.2. „Stiprinti Lietuvos

kibernetinės erdvės saugumą“, analizuojant vertinimo kriterijus nustatytinos sąsajos su PEF, Linkov, NIST atsparumo matricos Socialinės dimensijos Planavimo- pasirengimo dalies pirmojo punkto uždavinį, kuris atspindimas vertinimo kriterijumi – „Veikiančių ir tarpusavyje bendradarbiaujančių CERT veiklą vykdančių reagavimo į incidentus grupių skaičius“ (eilės Nr. 50). Taip pat įvairių dimensijų detektavimo dalį apimantis vertinimo kriterijus – „Sukurta nacionalinė išankstinio perspėjimo apie tinklų ir informacijos saugumo pažeidžiamumus ir grėsmes sistema“ (eilės Nr. 51). Pažymėtina, kad vienas iš El. informacijos saugos programos 3.2 uždavinio įgyvendinimo vertinimo kriterijų akcentuoja neteisėtos veiklos kibernetinėje erdvėje skaitmeninių įrodymų analizės laboratorijų formavimą. Toks poreikis buvo išsakytas E3 eksperto, ekspertinio interviu metu. Nagrinėjant El. informacijos saugos programos 3.3 uždavinį „Užtikrinti Lietuvos kompiuterių tinklo (virtualaus perimetro) apsaugą nuo išorinių kibernetinių atakų“ įgyvendinimo kriterijus: „Paskirta institucija, atsakinga už virtualų Lietuvos kibernetinės erdvės perimetrą sudarančias jungtis valdančių operatorių priežiūrą“ (eilės Nr. 55); „Kolektyvinės kibernetinėje erdvėje teikiamų paslaugų saugos įgyvendinimo ir kontrolės sistemos saugomų ir kontroliuojamų paslaugų dalis, procentais“ (eilės Nr. 58), nustatyta sąsaja su PEF, Linkov, NIST kibernetinio atsparumo matricos Fizinės ir Informacinės dimensijų Detektavimo dalių uždaviniais nusakančiais fizinių aplinkų bei išorinių paslaugų teikėjų stebėseną. Socialinės PEF, Linkov, NIST dimensijos Planavimo-pasirengimo septintasis uždavinys akcentuojantis kibernetinio saugumo teisinių ir reglamentavimo reikalavimo suvokimą sietinas su El. informacijos saugos programos pasiekimų vertinimo kriterijumi – „Sukurtos teisinės prielaidos ir patvirtinti tarptautinių tinklo jungčių įrengimo ir tolesnio jų valdymo reikalavimai, numatantys tokių tinklo jungčių operatorių atsakomybę už šių jungčių stebėjimo ir išankstinio perspėjimo, taip pat operatorių veiksmų koordinavimą, įvykus išorinei kibernetinei atakai“ (eilės Nr. 54). 24 paveiksle pateikiama apibenrinta El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos analizė pateikiama 24 paveiksle.

	Planavimas / pasirengimas	**Detektavimas**	**Absorbavimas**	**Atsistatymas**	**Adaptacija**
Fizinė	0	1	0	0,5	0
Informacinė	1	1	0	0,5	0
Kognityvinė	1	0,5	0	0,5	0
Socialinė	1	0,5	0	0,5	0

Šaltinis: *parengta autoriaus*

24 pav. *Atsparumo principų perkėlimas į LR teisės aktus – El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programa*

Kaip matoma paveiksle, labiausiai El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programoje daugiausiai apimamos Informacinės, Kognityvinės, Socialinės dimensijų Planavimo-pasirengimo fazei bei Fizinės ir Informacinės dimensijų Detektavimo fazei. Tačiau visiškai nenumatytos visų dimensijų Absorbavimo ir Adaptacijos fazės, beveik nenumatyta visų dimensijų Atsistatymo fazė. Darytina išvada, kad įvertinus el. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programą naudojant

PEF, Linkov, NIST atsparumo matricą, nustatyta, kad El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programoje reglamentuojama tik dalis kibernetinio atsparumo komponentų.

Bendrųjų elektroninės informacijos saugos reikalavimų aprašas. Bendrųjų elektroninės informacijos saugos reikalavimų aprašo paskirtis – sudaryti sąlygas saugiai automatizuotai tvarkyti valstybės registrų ir žinybinių registrų bei valstybės IS ir kitų IS informaciją. Apraše įtvirtintos nuostatos netaikomos tik įslaptintos informacijos tvarkymui. Visos kitos informacijos tvarkymui institucijų steigiamoms IS ir registrams aprašo nuostatos yra privalomos (Bendrųjų el. informacijos saugos reikalavimų aprašas, 2013). Trečiajame aprašo skyriuje, kuriame apibūdinami saugos organizavimo procesai, apibrėžiamos saugos įgaliotinio funkcijos, pagal kurių dalį, įgaliotinis „koordinuoja elektroninės informacijos saugos incidentų, įvykusių informacinėje sistemoje, tyrimą ir bendradarbiauja su kompetentingoms institucijoms, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės; organizuoja rizikos įvertinimą. Saugos įgaliotinis periodiškai organizuoja informacinės sistemos naudotojų mokymą elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas“ (Bendrųjų el. informacijos saugos reikalavimų aprašas, 2013). Vertinant šias funkcijas PEF, Linkov, NIST atsparumo matricos kontekste, pažymėtina, kad jos apima keletą PEF, Linkov, NIST atsparumo matricos dimensijų. Visų pirma, galima įžvelgti nemažai sąsajų su visų dimensijų adaptacijos dalimi, kuri apima po incidentinius veiksmus ir incidentų poveikio tyrimus. Taip pat galima identifikuoti ryšį su Socialinės dimensijos Planavimo-pasirengimo dalies punktais, apimančiais darbuotojų mokymus ir kibernetinio žinojimo kultūros formavimą. Ketvirtajame Bendrųjų el. informacijos saugos reikalavimų aprašo skyriuje, pagal jo pavadinimą turinčiame reglamentuoti incidentų valdymą, nustatoma IS naudotojų pareiga pranešti apie tai atsakingiems asmenims ir, kas ką turėtų informuoti incidentų atveju; plačiau apie incidentų valdymą šiame skyriuje nėra kalbama, todėl sunku vertinti iš jo naudingumo incidentų valdymui perspektyvos, tačiau galima būtų identifikuoti sąsajas su PEF, Linkov, NIST kibernetinio atsparumo matricos Socialinės dimensijos Detektavimo dalies punktais, apibrėžiančiais nustatytų įvykių komunikaciją suinteresuotoms šalims. Taip pat pats bandymas apibrėžti komunikavimo principus incidentų metu turi sąsajų su matricos Informacijos dimensijos Planavimo-pasirengimo antruoju uždaviniu, apibrėžiančiu būtinybę identifikuoti organizacinę komunikaciją ir informacijos srautus. Penktajame skyriuje „Rizikos vertinimas“ nustatoma saugos įgaliotinio funkcijos rizikų vertinimo procese. Pažymėtina, kad Bendrųjų el. informacijos saugos reikalavimų apraše pateikiama nuoroda į VRM išleistą metodinę priemonę „Rizikos analizės vadovas“, kuri kibernetinio saugumo srities ekspertų laikoma pasenusia. Rizikų vertinimo dalyje taip pat siūloma vadovautis konkrečiais Lietuvos ir tarptautiniais saugumo standartais, aprašomi svarbiausi rizikos veiksniai. Ketvirtojoje dalyje „Bendrųjų el.informacijos saugos reikalavimai“ nustatomi Informacinės sistemos veiklos tęstinumo valdymo plano turinio reikalavimai bei nuostatos, kad veiklos tęstinumo planas įsigalioja įvykus elektroninės informacijos saugos incidentui, informacinės sistemos naudotojų ir kitų asmenų įgaliojimai

ir veiksmai pagal planą įvykus elektroninės informacijos saugos incidentui bei iš atsparumo perspektyvos ypač svarbių kriterijų, pagal kuriuos galima nustatyti, ar informacinės sistemos veikla atkurta, į planą įeina skyrius 5.2. „Organizacines nuostatos“, kuriame turi būti nurodyta 5.2.1. „Informacinės sistemos veiklos tęstinumo valdymo grupės (toliau – veiklos tęstinumo valdymo grupė) sudėtis (vadovas, pavaduotojas ir kiti nariai)“. Šis punktas ir į punktą 5.2.2. „Veiklos tęstinumo valdymo grupės funkcijos“ patenkantis punktas 5.2.2.1. „Situacijos analizė ir sprendimų informacinės sistemos veiklos tęstinumo valdymo klausimais priėmimas“ sietinas su PEF, Linkov, NIST atsparumo matricos Kognityvinės dimensijos Atsistatymo dalies antruoju punktu „Atsistatymo sprendimų priėmimo protokolų nustatymas“. Punktas 5.2.2.2. „Bendravimas su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais“ sietinas su PEF, Linkov, NIST matricos Socialinės dimensijos atsistatymo dalies pirmuoju punktu „Viešųjų ryšių valdymas ir reputacijos atstatymas“. Veiklos tęstinumo plano punktas 5.2.2.3. „Bendravimas su susijusių informacinių sistemų veiklos tęstinumo valdymo grupėmis“ turi akivaizdžias sąsajas su PEF, Linkov, NIST atsparumo matricos Socialinės dimensijos Atsistatymo dalie antruoju punktu „Atsistatymo veiklų komunikavimas vidinėms suinteresuotoms šalims ir vykdomosios valdžios komandoms“. Taip pat šioje perspektyvoje vertintinas ir punktas 5.2.2.4. „Veiklos tęstinumo plano“, numatantis „bendravimą su teisėsaugos ir kitomis institucijomis, institucijos darbuotojais ir kitomis interesų grupėmis“.

Bendrųjų elektroninės informacijos saugos reikalavimų aprašo analizė pateikiama 25 paveiksle.

	Planavimas / pasirengimas	**Detektavimas**	**Absorbavimas**	**Atsistatymas**	**Adaptacija**
Fizinė	0	0	0	0	1
Informacinė	1	0	0	1	1
Kognityvinė	0	0	0	1	1
Socialinė	1	1	0	1	1

Šaltinis: *parengta autoriaus*

25 pav. *Atsparumo principų perkėlimas į LR teisės aktus – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas*

Kaip matoma paveiksle, labiausiai Bendrųjų elektroninės informacijos saugos reikalavimų apraše labiausiai apimamos visų dimensijų Adaptacijos fazė, Informacinės, Kognityvinės ir Socialinės dimensijų atsistatymo fazė, Socialinės dimensijos Planavimo-pasirengimo bei Detektavimo fazės bei Informacinės dimensijos Planavimo-pasirengimo fazė. Tačiau visiškai nenumatytos visų dimensijų Absorbavimo fazė, beveik nenumatyta visų dimensijų Detektavimo fazė. Darytina išvada, kad įvertinus Bendrųjų elektroninės informacijos saugos reikalavimų aprašą naudojant PEF, Linkov, NIST atsparumo matricą, nustatyta, kad Bendrųjų elektroninės informacijos saugos reikalavimų apraše reglamentuojama tik dalis kibernetinio atsparumo komponentų.

Nacionalinis kibernetinių incidentų valdymo planas. Nacionalinis kibernetinių incidentų valdymo planas nustato kibernetinio saugumo politiką įgyvendinančių institucijų, kitų viešojo administravimo subjektų, valdančių valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų

elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų ir viešojo administravimo subjektų, tvarkančių valstybės informacinius išteklius, veiksmus, atliekamus siekiant suvaldyti kibernetinius incidentus (Nacionalinis kibernetinių incidentų planas, 2016). Nacionaliniame kibernetinių incidentų valdymo plane kalbama apie tokių incidentų poveikį, kurie gali sutrikdyti ar sutrikdo valstybės informacinių išteklių, ypatingos svarbos informacinės infrastruktūros ir (ar) kitų elektroninių ryšių tinklų ir paslaugų ir (ar) informacinių sistemų darbą ir taip sukelti grėsmę nacionaliniam saugumui, žmonių sveikatai ar gyvybei, visuomenės gerovei ar valstybės funkcijų atlikimui, taip pat tarp institucinę kibernetinių incidentų valdymo sąveiką, kibernetinių incidentų klasifikavimo tvarką ir tarp institucinį bendradarbiavimą tiriant kibernetinius incidentus. Nacionaliniu kibernetinių incidentų valdymo plane taip pat nustatomos už kibernetinių incidentų valdymą atsakingos institucijos – Kibernetinio saugumo ir telekomunikacijų tarnyba prie KAM, vykdanti NKSC funkciją. Pagrindinė NKSC atsakomybių sritis – kai incidentas nustatomas valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje arba gali šias sistemas paveikti; visais kitais atvejais už incidentų valdymą atsakinga RRT.

Nagrinėjant Nacionalinį kibernetinių incidentų valdymo planą iš atsparumo perspektyvos ir sulyginant jame išdėstytus principus su PEF, Linkov, NIST atsparumo matricoje išdėstytomis atsparumo dimensijomis, galima identifikuoti Incidentų valdymo plano 12 punkto teigiančio, kad: „KIVT institucijos nedelsdamos, ne vėliau kaip per 30 minučių nuo kibernetinio incidento aplinkybių aptikimo, pateikia informaciją apie galimą kibernetinį incidentą tvarkytojui, ypatingos svarbos informacinės infrastruktūros valdytojui, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui ir elektroninės informacijos prieglobos paslaugų teikėjui“ (Nacionalinis kibernetinių incidentų planas, 2016), sąsajos su PEF, Linkov, NIST atsparumo matricos Kognityvinės dimensijos Detektavimo dalies pirmuoju uždaviniu, teigiančiu būtinybę analizuoti detektuotus įvykius, siekiant nustatyti jų tikslus ir metodus. Šis punktas taip pat susijęs ir su Informavimo dimensijos antruoju uždaviniu, teigiančiu būtinybę efektyviai ir savalaikiai informuoti pateikti reikalingus duomenis suinteresuotoms šalims ir sprendimų priėmėjams. Reagavimas į incidentus aprašomas antrajame Incidentų valdymo skirsnyje, 17–34 punktuose, kuriuose apibrėžiami bendrieji informavimo apie incidentus principai ir institucijų atsakomybės, atsižvelgiant į incidento prigimtį ir sudėtingumo mastą. Visi šie žingsniai sietini su įvairiais PEF, Linkov, NIST atsparumo matricos Kognityvinės ir Socialinės dimensijų Absorbavimo dalies uždaviniais, pradedant nuo šiose dalyse aprašomų sprendimų priėmimo protokolų taikymu, baigiant identifikuotų ekspertų kontaktavimo principų nustatymu.

Trečiajame Nacionalinio kibernetinių incidentų valdymo plano skirsnyje aprašomas tarp institucinis bendradarbiavimas tiriant incidentus. Šiame skirsnyje išdėstyti principai glaudžiai siejami su PEF, Linkov, NIST atsparumo matricos visų dimensijų adaptavimosi dalimi. Pradedant Fizinės dimensijos Adaptavimosi dalies pirmuoju punktu „Paslaugos ar vertybės, arba sistemos, peržiūra ir įvertinimas po incidentų“, incidentų valdymo plane ji apibūdinama kaip: „Tvarkytojas, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas ar elektroninės informacijos prieglobos paslaugų teikėjas, kurio RIS nustatytas kibernetinis incidentas, išanalizavęs ir įvertinęs visą informaciją, susijusią su kibernetiniu incidentu, atliktus

veiksmus ir panaudotas priemones: 37.1. privalo imtis priemonių, kad būtų pašalintas RIS pažeidžiamumas; 37.2. įvertina RIS riziką ir (ar) atitiktį Vyriausybės nustatytiems ar Ryšių reguliavimo tarnybos patvirtintiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams“ (Nacionalinis kibernetinių incidentų planas, 2016). Kognityvinės dimensijos Adaptavimosi dalyje pirmuoju uždaviniu aprašoma būtinybė peržiūrėti sprendimų priėmimo, valdymo procesą. Nacionaliniame kibernetinių incidentų valdymo plane šie principai įtvirtinami per kibernetinius incidentus valdančiųjų ir tiriančiųjų institucijų užduotis: „36.1. nustačiusios nepakankamą teisinį reglamentavimą, keičia teisės aktus (inicijuoja teisės aktų pakeitimus), reglamentuojančius kibernetinį saugumą; 36.2. prireikus atnaujina (inicijuoja atnaujinimą) ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus; 36.3. įvertina organizacinių ir techninių kibernetinio saugumo užtikrinimo priemonių tobulinimo ar atnaujinimo poreikį, suplanuoja priemones šiam poreikiui patenkinti ir užtikrina jų įgyvendinimą“.

Nacionalinio kibernetinių incidentų valdymo plano analizės rezultatai pateikiami 26 paveiksle.

	Planavimas / pasirengimas	Detektavimas	Absorbavimas	Atsistatymas	Adaptacija
Fizinė	1	0,5	0	1	1
Informacinė	1	0,5	1	0,5	1
Kognityvinė	1	1	1	0,5	1
Socialinė	1	0,5	1	0,5	1

Šaltinis: *parengta autoriaus*

26 pav. *Atsparumo principų perkėlimas į LR teisės aktus - Nacionalinis kibernetinių incidentų valdymo planas*

Kaip matoma paveiksle, Nacionaliniame kibernetinių incidentų valdymo plane apimamos beveik visų dimensijų fazės. Pasigendama Fizinės dimensijos absorbavimo fazės. Kiek mažiau dėmėsio skiriama Fizinės, Informacinės ir Socialinės dimensijų Detektavimo fazei bei Informacinės, Kognityvinės ir Socialinės dimensijų Atsistatymo fazei. Darytina išvada, kad įvertinus Nacionalinį kibernetinių incidentų valdymo planą naudojant PEF, Linkov, NIST atsparumo matricą, nustatyta, kad Nacionaliniame kibernetinių incidentų valdymo plane reglamentuojama didžioji dalis atsparumo komponentų. Vertėtų pažymėti, kad nepaisant to, jog lyginant Nacionaliniame kibernetinių incidentų valdymo plane esančių detektavimo principų sąsajas su PEF, Linkov, NIST matrica, beveik visų dimensijų Detektavimo ir Atsistatymo fazė turi ne tokias ryškias sąsajas lyginant su kitomis fazėmis. Tačiau lyginant NIST parengtame Kompiuterių saugumo incidentų valdymo vadove esantį Incidentų valdymo gyvavimo ciklą, akivaizdu, kad cikle esantys Detektavimo ir atsistatymo principai į Nacionalinį kibernetinių incidentų valdymo planą yra perkelti[34].

Apibendrinta atsparumo principų perkėlimo analizė pateikiama 27 paveiksle.

34 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

	Planavimas / pasirengimas	Detektavimas	Absorbavimas	Atsistatymas	Adaptacija	Dimensijų indeksas
Fizinė	1,5	3	0,5	2	2,5	9,5
Informacinė	5	2	1	2	3,5	13,5
Kognityvinė	3,5	2	1	2	2	10,5
Socialinė	5	2,5	1	2	3	13,5
	15	**9,5**	**3,5**	**8**	**11**	

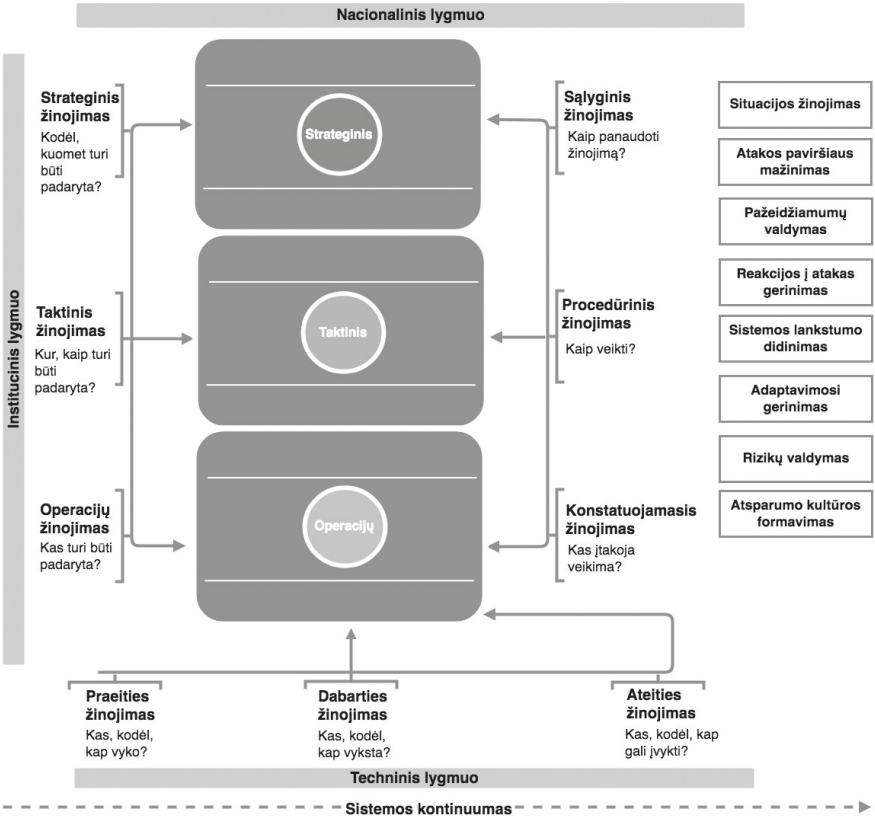
Šaltinis: *parengta autoriaus*

27 pav. *Atsparumo principų perkėlimas į LR teisės aktus - Apibendrintas atsparumo principų perkėlimo į LR teisės aktus indeksas*

Apibendrinant darytina išvada, kad kibernetinį saugumą reglamentuojančiuose LR teisės aktuose ryškiausia sąsaja darytina su PEF, Linkov, NIST atsparumo matricos Socialine ir Informacine dimensijomis, o mažiausia su Fizine ir Kognityvine. Atsižvelgiant į tai, kad technologinė dedamoji yra kiekvienu atveju specifinė kiekvienai organizacijai, daugiausia dėmesio vertėtų atkreipti į Kognityvinę dimensiją, t.y. kibernetinio saugumo situacijos, grėsmių, su šia sritimi susijusių priimamų sprendimų, ir kitų klausimų suvokimu. Reikia pažymėti, kad įvairūs kibernetinio suvokimo aspektai buvo ypač akcentuojami ir interviu dalyvavusių ekspertų. Taip pat atkreiptinas dėmesys, kad ypač mažai reglamentuoti visų dimensijų Absorbavimo fazės aspektai. Absorbavimą nemažai autorių (payzdžiui, Bruneau ir kt., 2003; Gao ir kt., 2011; Sansavini ir Nan, 2017) mato viena iš kertinių atsparumo sudedamųjų dalių.

3.10. Patikslintas kibernetinio atsparumo modelis

Atlikus ekspertų interviu, visi išskirti modelio konstrukciniai elementai patvirtinti. Kaip parodė Lietuvos Respublikos pagrindinių kibernetinį saugumą reglamentuojančių teisės aktų analizė, juose reglamentuota tik dalis atsparumo principų. Todėl, būtina siūlyti naujus mechanizmus, kurie galėtų papildyti esamų priemonių visumą, vienas jų – patikslintas ir papildytas organizacijų kibernetinio atsparumo kibernetinėms grėsmėms modelis, pateikiamas 28 paveiksle.



Šaltinis: *parengta autoriaus*

28 pav. *Patikslintas kibernetinio atsparumo modelis*

Tyrime dalyvavę ekspertai pabrėžė būtinybę vykdyti komunikaciją visomis organizacijos hierarchijos vertikalės kryptimis, todėl kibernetinio atsparumo modelyje skirtini trys organizacinės sistemos kibernetinio saugumo žinojimo ir bendradarbiavimo lygmenys: strateginis, taktinis ir operacijų. Nei viena valstybinė organizacija nevykdo savo veiklos vakuume, ji yra veikiama bendroje institucinėje sistemoje ir nacionaliniame kontekste vykstančių procesų. Organizacijos savo veiklas vykdo naudodamos IRT, dėl netinkamas jų organizavimo bei apsaugos kyla rizika, kad organizacijų veikla gali būti sutrikdyta. Šiems faktoriams apibrėžti modelyje išskiriami papildomi trys lygmenys: institucinis, nacionalinis ir technologijų. Ekspertų teigimu, kritiškai svarbūs elementai, siekiant padidinant organizacijos atsparumą, yra žinojimas ir komunikacija. Siekiant kuo geriau apimti žinojimo dimensijas, modelyje išskiriami devyni vienas kitą proceso dalyvių komunikacijos ir bendradarbiavimo metu papildantys žinojimo lygmenys:

- Organizacijos hierarchinio žinojimo lygmuo:
  - Strateginis žinojimo lygmuo – šiame lygmenyje formuojamas žinojimas, dėl ko vykdomos vienos ar kitos kibernetinio saugumo veiklos, nustatomos gairės jų įgyvendinimui.
  - Taktinis žinojimo lygmuo – formuojamas žinojimas apie priemones, kuriomis turėtų būti vykdomas strateginiame lygmenyje suformuotų užduočių įgyvendinimas.
  - Operacijų žinojimo lygmuo – konkrečių veiksmų įgyvendinimo žinojimas.
- Analitinis žinojimo lygmuo:
  - Praeities žinojimas – praėjusių kibernetinių grėsmių, incidentų, jų šalinimo būdų žinojimas, skaitmeninės ekspertizės (angl. *digital forensics*) veikla, po incidentinė peržiūra (angl. *post incident review*), išmoktų pamokų įvertinimas.
  - Dabarties žinojimas – stebėsena, įsibrovimo detektavimo sistemų informacijos valdymas, sistemos anomalijų analizė.
  - Ateities žinojimas – prognozavimas, nuspėjamoji duomenų analizė, ateities įžvalgos (angl. *foresight*).
- Meta-kognityvinis žinojimas (Schraw, 1998):
  - Sąlyginis žinojimas – žinojimas, kaip panaudoti turimas kibernetinio saugumo žinias.
  - Procedūrinis žinojimas – žinojimas, kaip vykdyti atliekamas užduotis iš kibernetinio saugumo perspektyvų.
  - Konstatuojamasis žinojimas – žinojimas, kaip padidinti turimas žinias, kokie faktoriai gali įtakoti žinių formavimą.

Taikant šį modelį, reikėtų įvertinti kiekvieną jo struktūrinį komponentą (situacijos žinojimas, atakos paviršiaus mažinimas ir kt.) visų žinojimo bei veiklos lygmenų kontekste.

IŠVADOS IR REKOMENDACIJOS

1-asis uždavinys. Atlikus mokslinių šaltinių analizę, siekiant atskleisti kibernetinių grėsmių dinamiką, kibernetinio saugumo ir atsparumo objektus, kibernetinio saugumo ir atsparumo valdymo ir organizacinius aspektus, formavimo prielaidas ir kliūtis, identifikuoti esminius faktorius, lemiančius kibernetinio saugumo aktualizavimą skirtinguose organizacijos valdymo lygmenyse, nustatyta:

1. Didėjant informacinių ir ryšio technologijų skverbčiai įvairiose žmonių veiklos srityse, intensyvėjant kibernetinėms atakoms didėja organizacijų patiriamos žalos mastas. Grėsmių poveikis stiprėja ne tik virtualiose, bet ir fizinėse aplinkose esančioms vertybėms ir infrastruktūroms; vis dažniau sutrikdoma valstybinių institucijų, ligoninių, finansų sektoriaus bei kritinių paslaugų teikimą vykdančių infrastruktūrų veikla. Tai sąlygoja būtinybę vertinti kibernetines grėsmes iš sisteminės perspektyvos, svarbus ne tik saugumo objekto suvokimo poslinkis nuo siauro technologinio požiūrio link įvairias valdymo sritis apimančios traktuotės, bet ir aktualizavimas bendrame nacionalinio saugumo lygmenyje.

2. Kibernetinio saugumo diskurse egzistuoja tam tikras terminijos sąmyšis – nėra pakankamai aiškių nusistovėjusių sąvokų. Su ankstyvajam saugumo laikotarpiui būdingais, tačiau vis dar vartojamais terminais, tokiais kaip informacinis saugumas, el. informacijos sauga, naudojamos ir vėlesniems saugumo laikotarpiams būdingos sąvokos: kibernetinis saugumas, kibernetinis incidentas. Todėl prieš egzistuojančią terminiją papildant naujais konceptais, būtina apibrėžti ir suvienodinti esamą sąvokų terminų sistemą, suformuoti jų konceptualias sąsajas.
3. Kibernetinio saugumo ir atsparumo reiškinių suvokimo plėtotė vyksta augant tam tikros saugumo bendruomenės kibernetinio saugumo raštingumo lygiui. Ypač svarbu, kad vartosenoje esantys kibernetinio saugumo apibrėžimai tam tikros kibernetinio saugumo bendruomenės atstovų būtų suprantami vienodai. Prieš vykdant bet kokį sąvokų kategorizavimą, būtina įvertinti, ar tai neturės neigiamo poveikio šių sąvokų apimamiems kibernetinio saugumo objektams, neįvyks konceptualus jų atskyrimas iš bendrojo saugos konteksto, nes tai galėtų sąlygoti neigiamas pasekmes šių objektų finansavimui, plėtrai, bendram jų svarbos vertinimui.
4. Kibernetinio atsparumo valdymo esmę sudaro aibė sisteminių veiksnių, tačiau esminiais komponentais laikytini adaptavimosi, absorbavimo ir atsistatymo gebėjimai, kurių ugdymas leidžia išvengti sistemos funkcionavimo poslinkio nuo judėjimo link nepageidaujamos sisteminės konfigūracijos, kai ji yra veikiama išorinio arba vidinio stresinio faktoriaus, planuoto ar neplanuoto pokyčio.
5. Vienas pagrindinių iššūkių formuojant kibernetinio saugumo sistemų atsparumą yra būtinybė užtikrinti šių sistemų apsaugai taikytų priemonių, jų efektyvumo ir kitų valdymo bei sisteminių parametrų slaptumą, tai sąlygoja informacijos silosą, gerosios praktikos dalinimosi trikdžius. Todėl, ypač svarbu užtikrinti tinkamą apsikeitimą informacija tarp organizacijos valdančiosios grandies ir kibernetinį saugumą užtikrinančių padalinių.
6. Nors kibernetinis atsparumas dažnai nagrinėjamas sudėtingų adaptyvių sistemų perspektyvoje, jam formuoti dažnai būtinas sisteminis, tarpsektorinis požiūris, tačiau jo plėtojimas turėtų būti vykdomas laikantis proporcingumo, priemonių adekvatumo ir sisteminio paprastumo principų.
7. Resursų paskirstymas ir veiklos prioritetų nustatymas turi tiesioginę įtaką kibernetiniam atsparumui, todėl kibernetinis atsparumas ir saugumas turėtų būti vertinami ir plėtojami lygiagrečiai su kitais organizacijos veiklos procesais. Nustatant finansavimo prioritetus, jiems turėtų būti suteikiamas toks pats svarbos lygmuo.
8. Atsparumo kaitos dinamika teigiamai įtakoja bendruosius organizacijos procesus, prisideda prie organizacijos evoliucionavimo. Kibernetinio atsparumo plėtrai organizacinių sistemų viduje svarbi tinkama ir savalaikė komunikacija, tarpinstitucinis bendradarbiavimas, aiškus veiklų pasidalijimas, dubliavimo vengimas. Taip pat labai svarbi kibernetinio atsparumo suvokimo sklaida, kuri turėtų būti vykdoma institucijų hierarchijos vertikale iš viršaus žemyn. Tinkamo lygio kibernetinio saugumo priemonių įgyvendinimas valstybinėse informacinėse sistemose didina piliečių pasitikėjimą valdžia, todėl aktuali ir išorinė komunikacija – kibernetinio

atsparumo plėtrai nacionaliniu mastu būtinas valdžios bendradarbiavimas su visuomene.

9. Siekiant konkretizuoti kibernetinio saugumo ir atsparumo reiškinius bei nustatyti jų konceptualias ribas, būtina plėtoti šios srities diskusiją tarp įvairias kompetencijų sritis atstovaujančių kibernetinio saugumo ekspertų. Siekiant nustatyti tolimesnes organizacijų kibernetinio atsparumo formavimo tendencijas, kibernetinių grėsmių transformacijos tendencijas bei identifikuoti naujus atsparumo taikymo modelius, rekomenduojama vykdyti nuolatinius, tarpdalykinius kibernetinio atsparumo srities tyrimus. Ypač rekomenduotinos absorbavimo reiškinio įvertinimo studijos.

2-asis uždavinys. Teorinių įžvalgų pagrindu formuojant konceptualų organizacinio atsparumo kibernetinėms grėsmėms modelį, integruojantį svarbiausius organizacijų kibernetinio atsparumo sisteminius ir valdymo faktorius, nustatyta:

1. Organizacinio ir sistemų atsparumo sričių konceptai yra mobilūs, todėl didžioji dalis šių sričių atsparumo formavimo principų taikytini formuojant kitų domenų atsparumo modelius.
2. Nepaisant to, kad pastaruoju metu ryšio ir komunikacijų technologijos yra pakankamai išplėtotos, egzistuoja informacinių silososų, kuriuose izoliuojami ne tik bendriniai informaciniai srautai, bet ir su kibernetiniu saugumu susijusi informacija, išlikimo tendencija. Todėl, vienas svarbiausių uždavinių organizacijų kibernetiniam atsparumui didinti – kibernetinio saugumo situacijos žinojimo gerinimas.
3. Organizacijos išgyvenimui grėsmę keliančių kritinių pažeidžiamumų identifikavimas, proaktyvus jų valdymą ir su jais susijęs reagavimas yra lemiami veiksniai siekiant užtikrinti tinkamą veiklos tęstinumo ir krizių valdymo srityje.
4. Vienas pagrindinių atsparumo principų yra adaptyvumas, kurio ugdymas gerina organizacijos gebėjimus judėti nuo reaktyvaus atsako link proaktyvaus pasirengimo ir gebėjimo veikti didelio nežinomumo sąlygomis.
5. Sistemos lankstumas – vienas esminių, sistemos atsparumą užtikrinančių faktorių, papildančių jos gebėjimą adaptuotis prie kibernetinių grėsmių, pertvarkant procesus bei sistemas pagal egzistuojančius kibernetinio saugumo situacijos poreikius.
6. Atsižvelgiant į kibernetinių atakų įvairialypę prigimtį, organizacijos atakos paviršiaus mažinimas turi būti vykdomas kompleksiškai, integruojant sisteminius ir žmogiškuosius faktorius.
7. Vykstant vis glaudesnei socio-fizinių ir techninių sistemų konvergencijai, reakcijų į atakas procesų gerinimas yra ypač aktualus sisteminio atsparumo komponentas.
8. Kylantis kibernetinių sistemų ir joms kylančių grėsmių sudėtingumo lygis reikalauja organizacinių bei techninių rizikų ir atsparumo valdymo procesų integracijos.

3-iasis uždavinys. Validuojant konceptualųjį organizacinio atsparumo kibernetinėms grėsmėms modelį ir identifikuojant svarbiausius jo konstrukcinius elementus, atliekant pusiau struktūrizuotą kibernetinio saugumo ekspertų interviu bei kokybinę Lietuvos kibernetinį saugumą reglamentuojančių teisės aktų analizę, nustatyta:

1. Pradiniai pateikto kibernetinio atsparumo modelio komponentai: kibernetinio saugumo situacijos žinojimo gerinimas, esminių pažeidžiamumų valdymo gerinimas, adaptyvių gebėjimų gerinimas, sistemos lankstumo gerinimas, reakcijos į atakas gerinimas, atakos paviršiaus mažinimas, rizikų valdymo gerinimas, yra validūs ir taikytini formuojant konceptualųjį organizacinio atsparumo kibernetinėms grėsmėms modelį.
2. Vertinant iš žmogiškųjų kibernetinio saugumo situacijos žinojimo perspektyvų, situacijos žinojimo gerinimas turėtų būti įgyvendinamas vykdant visų grandžių darbuotojų mokymus, paremtus praktiniais kibernetinio saugumo pavyzdžiais ir aktyviu jų dalyvavimu realiomis situacijomis bei suformuotais situacijos paaiškinimais paremtose pratybose.
3. Siekiant įgyvendinti tinkamus pasirengimo atakoms mechanizmus, būtina žinoti ne tik dabartinę kibernetinio saugumo situaciją, bet ir gebėti numatyti galimas kibernetinio saugumo grėsmes ateityje, rekomenduojama suformuoti kibernetinių grėsmių analizės mechanizmus valstybės mastu, padėsiančius prognozuoti potencialias grėsmes ir atsižvelgiant į gautą informaciją proaktyviai formuoti kibernetinės gynybos elementus.
4. Ypač svarbus veiksnys bendram kibernetinio saugumo situacijos žinojimui yra geopolitinės informacijos vertinimo mechanizmų diegimas, skirtų stebėti geopolitinę situaciją iš kibernetinio saugumo perspektyvos. Taip pat būtina vykdyti sisteminę kibernetinių nusikaltėlių, jų organizacijų stebėseną. Rekomenduojama suformuoti šias funkcijas vykdantį organizacinį vienetą, kuris pagal kompetenciją dalintųsi informacija su suinteresuotomis šalimis.
5. Siekiant didžiausio esminių pažeidžiamumų valdymo efekto organizacijoje, esminių pažeidžiamumų suvokimas turi būti formuojamas aukščiausiu tam tikros organizacijos valdymo lygmeniu, aiškiai pozicionuojant pažeidžiamumo objektus visoje būtinų apsaugoti elementų sistemoje.
6. Visų esminių pažeidžiamumų valdymo gerinimo priemonių aibėje būtina akcentuoti personalo mokymus, kurių pagalba būtų ugdoma bendra organizacijos, sektoriaus ar valstybės kibernetinio saugumo kultūra bei mokoma tinkamos kibernetinės higienos palaikymo ne tik sisteminiame, bet ir eilinio vartotojo lygmenyje.
7. Viena priemonių pažeidžiamumų valdymui gerinti – tai vertybių inventorizacijos ir sąrašų sudarymo vykdymas organizacijoje, jų tarpusavio sąsajų suvokimas. Esminių pažeidžiamumų valdymo poreikiai geriausiai perteikiami per jų sąsajas su organizacijos vykdoma veikla bei finansine dedamąja – tuomet atsiranda svarus, gerai visoms organizacijos grandims suvokiamas pagrindimas egzistuojantiems poreikiams.
8. Pakankamo esminių pažeidžiamumų valdymo svarbos nesuvokimas kelia dvejopas problemas:
    - egzistuoja tikimybė nesulaukti pritarimo, kad būtina šalinti pažeidžiamumus;
    - egzistuoja atvirkštinės manipuliacijos tikimybė, t.y. investicijų skyrimas ten, kur jų visai nereikėtų.

9. Esminių pažeidžiamumų valdymui būtina pasiekti konsensą ir bendrą situacijos suvokimą tarp IT padalinių, atliekančių sistemos tvarkymą ir sistemos valdytojo, pavyzdžiui, ministerijos; būtinas vienodas suvokimas, kad, visų pirma, turėtų būti vykdomas silpnų vietų šalinimas, o tik vėliau – plėtra. Saugos priemonių plėtojimą visų tipų organizacijose rekomenduojama vykdyti bent jau lygiagrečiai su plėtra, o ne po jos.
10. Adaptacijos gerinimo procesai turėtų prasidėti prieš įvykstant krizinėms situacijoms ar organizacijos teikiamų paslaugų lygio nuosmukiams. Dalis adaptacijos mechanizmų rekomenduojama atspindėti veiklos tęstinumo planuose, numatant scenarijus, apibrėžiančius visas galimas veiklos kryptis krizinių situacijų atvejais; rekomenduojama vykdyti esamų veiklos tęstinumo priemonių tobulinimą.
11. Vienas efektyviausių adaptavimosi gerinimo priemonių – pratybos, iš jų ir veiklos atkūrimo bei atsistatymo iš atsarginių kopijų pratybos. Siekiant padidinti pratybų vykdymo efektyvumą, būtina tobulinti pratybų atlikimo mechanizmus ir taip sumažinti vidinį pasipriešinimą dėl darbuotojų laiko gaišinimo ir dėl pratybų atsiradusių papildomų užduočių. Vertinant bendrąsias adaptavimosi tendencijas Lietuvoje, reikėtų konstatuoti, kad organizacijoms labiau būdinga reaguoti nei adaptuotis ar pasirengti. Ši sritis tobulintina kartu su po incidentinių įvykių peržiūra.
12. Sistemos lankstumui užtikrinti ypač svarbus elementas yra žmogiškasis faktorius, taigi kiek žmogus išliks rigidiškas savo požiūriais, ketinimais ir t.t., tiek nelanksti bus ir sistema. Sistemos lankstumui taip pat ypač svarbi organizacijos vadovybės kompetencija, nes, priešingu atveju, nekompetentingas vadovas gali duoti nurodymus sistemose naudoti esamus komponentus, kurie galbūt visiškai netinkami jos lankstumui ir atsparumui gerinti.
13. Bandymas pasiekti lankstumą atnaujinamose, iš prigimties statiškose sistemose gali duoti neigiamų rezultatų, todėl norint sistemas suformuoti lanksčiomis, rekomenduojama jas kurti iš pagrindų, nes, priešingu atveju, rigidiškai sistemai pereiti iš statiškos į lanksčią bei suformuotą moduliais gali būti pernelyg sudėtinga.
14. Prieš priimant sprendimus dėl specifinių saugumo priemonių taikymo būtina įvertinti, ar ši priemonė pakankamai efektyvi atsakyti į egzistuojančius saugumo iššūkius, kai kibernetinė priešprieša tarp atakuojančiųjų ir besiginančiųjų šalių evoliucionuoja nuo paprasto kibernetinio incidento link sisteminių kibernetinių karinių veiksmų, todėl atsiranda poreikis konceptualiai pakelti reagavimo veiksmus į kibernetinės gynybos (angl. *cyber defence*) lygmenį.
15. Kritiškai svarbu reakcijai į atakas – saugumo politikos apibrėžimas organizacijoje; apibrėžtos reaguojant į atakas naudojamos įrangos taikymo procedūros.
16. Dažnai pernelyg didelis dėmesys skiriamas organizacijos atakos paviršiaus mažinimui iš išorinių grėsmių perspektyvos, tačiau dažnai neįvertinamas labai svarbus ir gana pažeidžiamas bei silpnas organizacinės sistemos elementas – žmogiškasis faktorius.
17. Augant socialinės inžinerijos atakoms ypač aktualūs yra darbuotojų mokymai ir jų švietimas, kuris, kartu su kibernetinės higienos ugdymu ir procedūriniais mechanizmais, yra viena iš pagrindinių priemonių atsižvelgiant į emocijomis

besivadovaujančių žmonių prigimtį. Mokymus rekomenduojama vykdyti sudarant galimybę personalui realiai sudalyvauti simuliuojamuose atakose, vėliau parodant rezultatus ir atrastas saugumo spragas; tokios priemonės turi potencialą tapti veiksmingesnėmis suvokimo apie kibernetinio saugumo būklę formavimui nei formalių mokymo metodų naudojimas.

18. Organizacijoje rizikų visumos valdymas yra vienas iš pagrindinių uždavinių, nepaisant kokio pobūdžio rizikos tai bebūtų. IT rizikos yra bendra visų rizikų dalis, tad jos valdymas turi būti integruotas į visų kitų organizacijai kylančių rizikų visumą; tik aukštą rizikų valdymo kultūrą turinti organizacija geba integruotai valdyti visas rizikas, jų nediversifikuodama. Atsižvelgiant į tendenciją, kad atsiranda atvejų, kai su į IT sritimi susijusias problemas kitos organizacijos dalys įsiklausyti nenori, rekomenduojama tai gerinti formuojant organizacijos kibernetinio saugumo kultūrą, požiūrį į kibernetinio saugumo keliamas problemas, didinant bendros kibernetinio saugumo problematikos suvokimą. Atsiradus suvokimui organizacijoje stiprėja rizikų valdymo ir kibernetinio saugumo gerinimo inercija. Rizikų valdymas turėtų egzistuoti sistemos palaikymo ir jos gyvavimo procesuose iki neigiamų veiksnių sukeliamo sistemos veiklą trikdančio poveikio ir būtent tinkamai atliktas rizikų valdymas padėtų sugrįžti jai į pradinę būseną.
19. Rizikų valdymas yra tiesiogiai susijęs su kompanijos, organizacijos, aljanso narių skirtingų padalinių gebėjimo bendradarbiauti ir keistis informacija. Tai apima informacijos sklaidą ir viešinimą apie procesus, vykdomas darbines veiklas, naudojamą įrangą ir kt. Jeigu šie procesai nevykdomi, organizacijos nariai nesupranta pavojų, jei šie pavojai tinkamai neįvertinami, yra sudėtinga apibrėžti rizikas, kurios galėtų atsirasti organizacijos sistemose, skirtingiems padaliniams vykdant tik jiems žinomas veiklas. Kuo daugiau personalas žinos kas vyksta, kokios sistemos dalyvauja ir kaip jos tarpusavyje susijusios, tuo bus geresnis rizikos valdymas. Taigi, rizikų valdymo vienas iš esminių uždavinių – įtraukti kuo daugiau žmonių į rizikos valdymo procesą iš skirtingų organizacijos veiklos sektorių, neapsiribojant vien IT. Viešajame sektoriuje Lietuvoje egzistuoja tendencija visus su kibernetinio saugumo sritimi susijusius rizikų valdymo veiksmus deleguoti IT padaliniams. Tačiau saugos ir IT padaliniai gali suteikti reikiamas pagalbines priemones, o IT rizikų vertinimą turi atlikti organizacijos veiklos procesus vykdanti jos dalis.
20. Pats rizikų valdymo procesas Lietuvos viešajame sektoriuje neblogai reglamentuotas, tačiau rekomenduojama atnaujinti metodines priemones; kasmet atliekami rizikų vertinimai ganėtinai formalūs; į bendrą rizikų procesą rekomenduojama įtraukti daugiau organizacijos atstovų, ne tik saugos įgaliotinius.
21. Vertinant iš atsparumo perspektyvos, Lietuvos Respublikos teisės aktuose, reglamentuojančiuose kibernetinį saugumą išsamiausiai apibrėžti atsparumo domeno planavimo ir pasirengimo principai; stokojama Absorbavimo, Detektavimo ir Atsistatymo dimensijas apimančių atsparumo nuostatų formalizavimo. Formuojant naujus kibernetinį saugumą reglamentuojančius teisės aktus, rekomenduojama didesnį dėmesį skirti kognityviniams atsparumo aspektams bei visų atsparumo dimensijų Absorbavimo, Detektavimo ir Atsistatymo fazėms.

LITERATŪRA IR KITI ŠALTINIAI

1. Adams J. Virtual Defense (2001, May 1). Foreign Affairs. Prieiga per internetą: https://www.foreignaffairs.com/articles/2001-05-01/virtual-defense.
2. Al-Kalbani A., Deng H., Kam B. (2014, December). A Conceptual Framework for Information Security in Public Organizations for E-Government Development – 25th Australasian Conference on Information Systems Information Security for E-Government, 2014, December 8–10, Auckland, New Zealand.
3. Allen, J. (2011). Measures for managing operational resilience. *EDPACS*, *44*(6), 1-6.
4. Andersen, K. V. (2006). E-government: Five Key Challenges for Management. The Electronic Journal of e-Government, 4(1), p. 1–8.
5. Augustinaitis A., Rudzkienė V., Petrauskas R. ir kt. (2009). *Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas*. Mykolo Romerio universitetas.
6. Ashenden, D. (2011, July). Cyber Security: Time for Engagement and Debate – in European Conference on Cyber Warfare and Security. Academic Conferences International Limited, p. 11.
7. Ayala, L. (2016). *Cybersecurity lexicon* (Vol. 158). Apress.
8. Backhouse, J. Dhillon, G. (1996). Structures of Responsibility and Security of Information Systems. European Journal of Information Systems, 5, p. 2–9.
9. Balutis, A., Cho, A., Stewart-Weeks, M., & Willis, S. (2016). Architecting Resilience: Perspectives From Public Sector Leaders.
10. Barlow J. (2010). Cyber War and U.S. Policy: Part I, Neo-Realism. Interface: e-Journal of Education, Community and Values, 10(5).
11. Bartel, A., Klein, J., Traon, Y. L. Monperrus M. (2012). Automatically Securing Permission-Based Software by Reducing the Attack Surface: An Application to Android – Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering, p. 274–277.
12. Bartol, N., Bates, B., Goertzel, K. M., & Winograd, T. (2009). Measuring Cyber Security and Information Assurance: A State-of-the-Art Report. Information Assurance Technology Analysis Center IATAC.
13. Baskerville, R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development. ACM Computing Surveys, 25(4), p. 375–414.
14. Ben-Israel, I., & Tabansky, L. (2011). An Interdisciplinary Look at Security Challenges in the Information Age. Military and Strategic Affairs, 3, p. 21–37.
15. Bendrath R. (2001). The Cyberwar Debate: Perception and Politics In US Critical Infrastructure Protection. Information and Security: An International Journal (7), p. 80–103.
16. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, Nr. 716, 2013 m. liepos 24 d., Vilnius.
17. Berkes, F. (2007). Understanding Uncertainty and Reducing Vulnerability: Lessons From Resilience Thinking. Natural Hazards, 41(2), p. 283-295.

18. Birchall, D., Ezingeard, J. N., McFadzean, E., Howlin, N., & Yoxall, D. (2004). Information Assurance: Strategic Alignment and Competitive Advantage. Grist Ltd.
19. Bishop, M., Carvalho, M., Ford, R., Mayron, L. (2011). Resilience is More Than Availability. Proceedings of the New Security Paradigms Workshop (NSPW), p. 95–104.
20. Björck F., Henkel M., Stirna J., Zdravkovic J. (2015). Cyber Resilience – Fundamentals for A Definition – *Rocha Á. et al. New Contributions in Information Systems and Technologies, 311, Advances in Intelligent Systems and Computing*, *Berlin: Springer*, 353, p. 311–316.
21. Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. In New Contributions in Information Systems and Technologies. Springer, Cham, p. 311–316.
22. Board Briefing on IT Governance (2001) IT Governance Institute. Prieiga per internetą: https://www.oecd.org/site/ictworkshops/year/2006/37599342.pdf
23. Bodeau, D. J., Graubart, R. D., Laderman, E. R. (2014). Cyber Resiliency Engineering Overview of the Architectural Assessment Process. Procedia Computer Science, 28, p. 838–847.
24. Bodeau, D., Graubart, R. (2016). Cyber Resilience Metrics: Key Observations. MITRE.
25. Bodeau, D., Graubart, R., Picciotto, J., McQuaid, R. (2012). Cyber Resiliency Engineering Framework (2012).
26. Bordens, K.S., Abbott, B.B. (2010). Research Design and Methods: A Process Approach, 8th edition, New York: McGraw-Hill, p. 146.
27. Bourbeau P. (2013). Resiliencism: Premises and Promises In Securitization Research. Resilience: International Policies, Practices, and Discourses, 1(1), p. 3–17.
28. Bourbeau, P. (2013). Resiliencism: Premises and Promises in Securitisation Research. Resilience, 1(1), p. 3–17.
29. Brackney, R. (1998, October, 23). Cyber-Intrusion Response. Reliable Distributed Systems – *Proceedings, Seventeenth IEEE Symposium*.
30. Brand, F., & Jax, K. (2007). Focusing the meaning(s) of Resilience: Resilience As A Descriptive Concept and a Boundary Object. Ecology and Society, 12(1).
31. Brassett J., Croft S., Vaughan-Williams N. (2013). Introduction: an Agenda for Resilience Research in Politics and International Relations. Politics, 33(4), p. 221–228.
32. British Standards Institution (1995), 1995BS 7799-1:1995. Information Security Management. Code of Practice for Information Security Management Systems. BSI.
33. Bruneau, M., Chang, S. E., Eguchi R.T., Lee, G. C, O'Rourke, T.D., Reinhorn, A. M., Shinozuka, M., Tierney, K., Wallace, W. A., Winterfeldt D. (2003). A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earth Spectra. 19(4), p.733–752.

34. Bryant W. (2015). Cyberspace Resiliency: Springing Back With The Bamboo. M. Blowers (ed.), Evolution of Cyber Technologies and Operations to 2035.
35. Bryman A. (2012). Social Research Methods. 4th edition, Oxford: Oxford University Press, p. 160.
36. Bulgurcu, B., Cavusoglu, H., and enbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS quarterly, 34(3), p. 523–548.
37. Buzan, B., Wæver O., Wilde J., (1998). Security: A New Framework for Analysis Boulder: Lynne Rienner Publishers.
38. Byrnes, F. C., & Proctor, P. (2002). Information Security Must Balance Business Objectives. Prieiga per internetą: http://www.informit.com/articles/article.aspx?p=26952
39. Camp, L. J. Lewis, S. (2005). Economics of Information Security. Ethics and Information Technology, 7, p. 61–73.
40. Carlson, J. M., & Doyle, J. (1999). Highly Optimized Tolerance: A Mechanism for Power Laws in Designed Systems. Physical Review E, 60(2), 1412.
41. Cavelty, M. D. (2010). The Reality and Future of Cyberwar. Zurich, Switzerland: CSS Analysis in Security Policy.
42. Chandra et al. (2010). Understanding Community Resilience In The Context of National Health Securit. RAND.
43. Chaves, A., Rice, M., Dunlap, S., Pecarina, J. (2017). Improving the Cyber Resilience of Industrial Control Systems. International Journal of Critical Infrastructure Protection, 17, p. 30–48.
44. Chen D., Zhao G. (2012). Data Security and Privacy Protection Issues in Cloud Computing. International Conference on Computer Science and Electronics Engineering.
45. Christianson, M. K., Farkas, M. T., Sutcliffe, K. M., & Weick, K. E. (2009). Learning Through Rare Events: Significant Interruptions at the Baltimore & Ohio Railroad Museum. Organization Science, 20(5), 846-860.
46. Corey, T. Holzer, J. E. (2016). The Ethics of Hacking Back. CERIAS Tech Report. Lerums Center for Education and Research Information Assurance and Security Purdue University, West Lafayette.
47. Craigen, D., Diakun-Thibault, N., Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10).
48. Crosbie M., Spafford H. E. (1995). Applying Genetic Programming to Intrusion Detection. AAAI Technical Report, FS-95-01.
49. Cyberspace Ooperations. (2013). Joint Publication, 3–-12 (R). Prieiga per internetą: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.
50. Dahlman O. (2011). Security and Resilience. Resilience: Interdisciplinary Perspectives on Science and Humanitarianism, (2).
51. Dean, M. (2012). Rethinking Neoliberalism, Journal of Sociology, 50(2).

52. Dekker, S., Hollnagel, E., Woods, D., & Cook, R. (2008). Resilience Engineering: New Directions for Measuring and Maintaining Safety in Complex Systems. Lund University School of Aviation.
53. Demos (2010) Edwards C. Resilient Nation. London: Demos.
54. Derian, J. (2000). Virtuous War/Virtual Theory. International Affairs, 76(4), p. 71–88.
55. Deswarte Y., Laurent Blain L., Fabre J. (1991). Intrusion Tolerance in Distributed Computing Systems. IEEE Xplore Conference: Research in Security and Privacy, Proceedings.
56. Dhillon G., Backhouse J. (2000). Information System Security Management in the New Millennium. Communications of the ACM, 43(7).
57. Dhillon, G., Backhouse, J. (2001). Current Directions in IS Security Research: Towards Socio-Organizational Perspectives. Information Systems Journal, 11(2), p. 127–153.
58. Diep N.N., Hung L. X., Zhung Y., Lee S., Lee Y.K., Lee H. (2007). Enforcing Access Control Using Risk Assessment. Proceedings of the Fourth European Conference on Universal Multiservice Networks (ECUMN'07).
59. Doyle, M. W. (1998). Ways of War and Peace. New York: Norton.
60. Duffield, M. (2011). Environmental Terror: Uncertainty, Resilience and the Bunker. Global Insecurities Centre, p. 6–11.
61. Duffield, M.R. (2012) Challenging Environments: Danger, Resilience, and the Aid Industry. Security Dialogue 43(5), p. 475–492
62. Duggan, P. M. (2015). Strategic Development of Special Warfare in Cyberspace. Joint Force Quarterly, 79(4).
63. Edelman, M. (1977). Political Language: Words that Succeed and Policies that Fail. New York: Academic Press.
64. Edelman, M. (1985). The Symbolic Uses of Politics: With A New Afterword. Urbana: University of Illinois Press.
65. Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programa, Nr. 796, 2011 m. birželio 29 d., Vilnius.
66. Elman C. (2008). Realism – *Security Studies: An introduction. Williams P. D. London: Routledge*, p. 15–28.
67. Eloff, J. H., & Eloff, M. (2003, September). Information Security Management: A New Paradigm – In Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement Through Technology. South African Institute for Computer Scientists and Information Technologists, p. 130–136.
68. Endsley M.R., Bolte B., Jones D.G. (2003). Designing for Situation Awareness: An Approach to User-Centered Design. Boca Raton: CRC press.
69. Eriksson J., Giacomello G. (2006, July). The Information Revolution, Security, and International Relations: (IR) Relevant Theory? – *International Political Science Review/Revue internationale de science politique*, 27(3), p. 22–244.

70. Eriksson J., Giocomello G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? International Political Science Review, 27 (3), p. 221–244.
71. Eriksson, J. (2001). Securitizing IT. Threat Politics: New Perspectives on Security, Risk and Crisis Management. p.145-163.
72. Ernest Chang, S., & Ho, C. B. (2006). Organizational Factors to The Effectiveness of Implementing Information Security Management. Industrial Management & Data Systems, 106(3), p. 345–361.
73. Everard, J. (2000). Virtual States: The Internet and The Boundaries of The Nation-State. London: Routledge.
74. Ezingeard, J. N., & Bowen-Schrire, M. (2007). Triggers of Change in Information Security Management Practices. Journal of General Management, 32(4), p. 53–72.
75. Fazlida, M. R., Said, J. (2015). Information Security: Risk, governance and implementation setback. Procedia Economics and Finance, 28, p. 243–248.
76. Fjäder, C. (2014). The Nation-State, National Security and Resilience in The Age of Globalisation. Resilience, 2(2), p. 114–129.
77. Flynn S. A (2011). National Security Perspective on Resilience. Interdisciplinary Perspectives on Science and Humanitarianism, (2).
78. Ford, R., Carvalho, M., Mayron, L., Bishop, M. (2012). Towards Metrics for Cyber Security – Proceedings of the 21st EICAR Annual Conference, p. 151–159.
79. Friedberg, I., Mclaughlin, K., Friedberg, I., Mclaughlin, K., Smith, P., Wurzenberger, M. (2016). Towards a Resilience Metric Framework for Cyber-Physical Systems, ICS-CSR, 2016 (2014), p. 19–22.
80. Galatenko V. (2006). *Стандарты информационной безопасности*. Интернет-Университет Информационных Технологий.
81. Gao, J, Buldyrev, SV, Havlin, S., Stanley H. E. (2011). Robustness of A Network of Networks. Phys Rev Lett (2011).
82. Gebauer, J., Schober, F. (2006). Information System Flexibility and the Cost Efficiency of Business Processes. Journal of the Association for Information Systems, Vol. 7, No. 3, p. 122–147.
83. Georgia Institute for Information Security & Privacy 2016. Emerging Cyber Threats Report. Prieiga per internetą:
84. http://www.iisp.gatech.edu/sites/default/files/documents/2016_georgiatech_cyberthreatsreport_onlinescroll.pdf .
85. Gerasimov, V. (2013). Ценность науки в предвидении. Новые вызовы требуют переосмыслить формы и способы ведения боевых действий, 2013. Prieiga per internetą: http://www. vpk-news. ru/articles/14632.
86. Ghernaouti S. (2013). Cyber Power: Crime, Conflict and Security in Cyberspace (Forensic Sciences). Lausanne: EPFL Press.
87. Gibson, C. A., Tarrant, M. (2010). A Conceptual Models approach to organisational resilience. The Australian Journal of Emergency Management, 25(02).
88. Gitz, V., Meybeck, A. (2012, April 24). Risks, Vulnerabilities and Resilience in A Context of Climate Change. Building Resilience for Adaptation to Climate Change in the Agriculture Sector – *Proceedings of A Joint FAO/OECD Workshop*.

89. Goldman, H. G. (2010). Building Secure, Resilient Architectures for Cyber Mission Assurance. Secure and Resilient Cyber Architectures Conference MITRE, p. 1–18.
90. Goodin, R. E. (2010). The Oxford Handbook of International Relations Oxford: Oxford University Press. p. 133.
91. Grobler, M., van Vuuren, J. J., & Zaaiman, J. (2011, July). Evaluating Cyber Security Awareness in South Africa. In European Conference on Cyber Warfare and Security – Academic Conferences International Limited, p. 113.
92. Hale, A., Heijer, T. (2006). Defining Resilience – *Hollnagel, E., Woods, D.D., Leveson, N. (Eds.), Resilience Engineering: Concepts and Precepts. Ashgate Publishing Limited, Aldershot*, p. 35–40.
93. Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and The Copenhagen School. International studies quarterly, 53(4), p. 1155–1175.
94. Häring, I., Ebenhöch, S., & Stolz, A. (2016). Quantifying Resilience for Resilience Engineering of Socio Technical Systems. European Journal for Security Research, 1(1), p. 21–58.
95. Häring, I., Sansavini, G., Bellini, E., Martyn, N., Kovalenko, T., Kitsak, M., Linkov, I. (2017). Towards A Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures, and Case Studies – *Resilience and Risk*. *Dordrecht: Springer*, p. 21–80.
96. Hart, C. (2011, May 12-15). Mobilizing the Cyberspace Race: the Securitization of the Internet and its Implications for Civil Liberties. Cyber-Surveillance in Everyday Life: An International Workshop, p. 13.
97. Havlin, S., Kenett, D. Y., Ben-Jacob, E., Bunde, A., Cohen, R., Hermann, H., Portugali, J. (2012). Challenges in Network Science: Applications to Infrastructures, Climate, Social Systems and Economics. The European Physical Journal Special Topics, 214(1), p. 273–293.
98. Heinimann, H. R., Hatfield, K. (2017). Infrastructure Resilience Assessment, Management and Governance-State and Perspectives – *Resilience and Risk*. *Springer, Dordrecht*, p. 147–187.
99. Herrington, L., Aldrich, R. (2013). The Future of Cyber-Resilience in An Age of Global Complexity. Politics, 33(4), p. 299–310.
100. Hitchings, J. (1996). A Practical Solution to The Complex Human Issues of Information Security Design – *Information Systems Security: Facing the Information Society of the 21st Century. Katsikas S.K. & Gritzalis, D. (eds)*, p. 3–12.
101. Holling C.S. (1973). Resilience and Stability of Ecological Systems. Annual Review of Ecology and Systematics. (4), p. 1–23.
102. Hollnagel, E., Woods, D. D. (2006). Resilience Engineering: Concepts and Precepts. Ashgate.
103. Holzer, C. T., & Lerums, J. E. (2016, May). The Ethics of Hacking Back – *Technologies for Homeland Security (HST), 2016 IEEE Symposium, IEEE*, p. 1–6.
104. Hong K., Chi Y; Louis R Chao L R., Jih-Hsing Tang J. An Integrated System Theory of Information Security Management Information Management & Computer Security (2003). Information and Computer Security.

105. Houston Jr., C. J., Sicker, D. C. (2014). Maturity and Process Capability Models and Their Use in Measuring Resilience in Critical Infrastructure Protection Sectors. International Journal of Strategic Information Technology and Applications, 5(2), p. 44–63.
106. Hubbard D. Seiersen R. How to Measure Anything in Cybersecurity Risk (2016). New Jersey: John Wiley & Sons, Inc.
107. Hufty, M. (2011). Investigating Policy Processes: The Governance Analytical Framework (GAF).
108. Ignatiadis, I., Nandhakumar, J. (2007). The Impact of Enterprise Systems on Organizational Resilience. Journal of Information Technology, 22(1), p. 36–43.
109. Jackson, M., Fitzgerald, J. S. Resilience Profiling in The Model-Based Design of Cyber-Physical Systems. Computing Science. Technical Report Series, CS-TR-1500.
110. Jagtman, H. M., Hale, A. R., & Heijer, T. (2006). Ex Ante Assessment of Safety Issues of New Technologies in Transport – *Transportation Research, part A: Policy and Practice*, 40(6), p. 459–474.
111. James, H. (1996). Managing Information Systems Security: A Soft Approach. Proceedings of the Information Systems Conference of New Zealand.
112. T. Janeliūnas (2007). *Komunikacinis saugumas*. VU leidykla, Vilnius.
113. JAV ginkluotųjų pajėgų Jungtinis operacijų štabas (2013). Prieiga per internetą: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf
114. Joint Chiefs of Staff, Joint Operations (2012), Information Operations, Washington DC: U.S. Government Printing Office, p. 3–13.
115. Joseph J. (2013). Resilience in UK and French Security Strategy: An Anglo-Saxon Bias? Politics, 33(4), p. 253–264.
116. Kallinikos, J. (2009). The Regulative Regime of Technology in ICT and Innovation in the Public Sector. Palgrave Macmillan, London, p. 66–87.
117. Katzenstein, P., Keohane, R.O., Krasner, S. (1998). International Organization and the Study of World Politics. International Organization 52(4), p. 645–85.
118. Kaufmann, M. (2015). Resilience Governance and Ecosystemic Space: A Critical Perspective on the EU Approach to Internet Security. Environment and Planning D: Society and Space, 33(3), p. 512–527.
119. Kendra, J. M., & Wachtendorf, T. (2003). Elements of Resilience After the World Trade Center Disaster: Reconstituting New York City‘s Emergency Operations Centre. Disasters, 27(1), p. 37–53.
120. Kenneally E. Bailey M. (2013). Cyber Security Research Ethics Dialogue and Strategy Workshop.
121. Kim, S. (2007). Governance of Information Security: New Paradigm of Security Management – *Computational Intelligence in Information Assurance and Security*. *Springer, Berlin, Heidelberg*, p. 235–254.
122. Kim, S., & Seong Leem, C. (2005). Enterprise Security Architecture in Business Convergence Environments. Industrial Management & Data Systems, 105(7), p. 919–936.

123. Kissel, R. (2013). Glossary of Key Information Security Terms, NIST IR 7298 National Institute of Standards and Technology (NIST), US Department of Commerce. Prieiga per internetą: http://csrc.nist.gov/publications.
124. Kling, R. (1980). Social Analysis of Computing: Theoretical Perspectives in Recent Empirical Research. ACM Computing Surveys, 12, p. 61–110.
125. Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson Ford, F. (2006). Information Security: Management's Effect on Culture and Policy. Information Management & Computer Security, 14(1), p. 24–36.
126. Knorr, K., and Röhrig, S. (2001). Security Requirements of e-Business Processes.
127. Kong, H.-K., Kim, T.-S. Kim, J. (2012). An Analysis on Effects of Information Security Investments: A BSC Perspective. Journal of Intelligent Manufacturing, 23(4), p. 941–953.
128. Kotulic, A. G., & Clark, J. G. (2004). Why There Aren't More Information Security Research Studies. Information & Management, 41(5), p. 597–607.
129. Kraemer S., Carayon P., Clem J. (2009). Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities. Computer Security, 28(7), p. 509–520.
130. Krotofil, M., & Cárdenas, A. A. (2013, October). Resilience of Process Control Systems to Cyber-Physical Attacks – *Nordic Conference on Secure IT Systems*, p. 166–182.
131. Kwon, J., Ulmer, J. R., & Wang, T. (2012). The Association Between Top Management Involvement and Compensation and Information Security Breaches. Journal of Information Systems, 27(1), p. 219–236.
132. Lakoff, A. and Collier, S. (2010). Infrastructure and Event in B. Braun and S. Whatmore (eds.), The Stuff of Politics: Technoscience, Democracy, and Public Life. Minneapolis: University of Minnesota Press.
133. Lallemant D. (2013). Building Post-Disaster Resilience: A Diagram. Prieiga per internetą: http://resilienturbanism.org/dlallemant/building-post-disaster-resilience-a-diagram/.
134. Landwehr, C. E. (2001). Computer Security. International Journal of Information Security, 1(1), p. 3–13.
135. Landwehr, C. E.; Heitmeyer, C. L., McLean, J. D. (2001). A Security Model for Military Message Systems: Retrospective.
136. Landwehr, Carl E. (1981). A Survey of Formal Models for Computer Security, NRL Report 8489. Washington D.C.: Naval Research Laboratory.
137. Layne, K., Lee, J. (2001). Developing Fully Fnctional E-government: A Four Stage Model. Government Information Quarterly, 18(2), p. 122–136.
138. Ledesma J. (2014). Conceptual Frameworks and Research Models on Resilience in Leadership, p. 1–8.
139. Lee, A. V., Vargo, J., & Seville, E. (2013). Developing A Tool to Measure and Compare Organizations' Resilience. Natural Hazards Review, 14(1), p. 29–41.
140. Lehto, M. (2013, July). The Ways, Means and Ends in Cyber Security Strategies – *Proceedings of the 12th European Conference on Information Warfare and Security (Jyväskylä, 2013), Academic Publishing, Reading*, p. 182–190.

141. Lehto, M. (2013). The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies. International Journal of Cyber Warfare and Terrorism (IJCWT), 3(3), p. 1–18.
142. Leiwo, J., Gamage, C., & Zheng, Y. (1999, September). Organizational Modeling for Efficient Specification of Information Security Requirements – *East European Conference on Advances in Databases and Information Systems. Springer, Berlin, Heidelberg*, p. 247–260.
143. Lewis, T. G., Mackin, T. J., Darken, R. (2011). Critical Infrastructure as Complex Emergent Systems. International Journal of Cyber Warfare and Terrorism, 1(1), p. 1–12.
144. Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. MIS quarterly, p. 71–90.
145. Lietuvos kibernetinio saugumo įstatymas, Nr. XII-1428, 2014 m. gruodžio 11 d., Vilnius.
146. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, Nr. XI-1807, 2011 m. gruodžio 15 d., Vilnius.
147. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas (2011), Nr. XI-1807.
148. Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., Kott, A. (2013). Resilience Metrics for Cyber Systems. Environment Systems and Decisions, 33(4), p. 471–476.
149. Liu Z., Yang D., Wen D., Zhang W., Mao W. (2011). Cyber-Physical-Social Systems for Command and Control. IEEE Intelligent systems, 26 (4), p. 92–96.
150. Liveri, D., Sarri, A., Skouloudi, C. (2015). Security and Resilience in eHealth. Enisa.
151. Lobato, L. C., & Kenkel, K. M. (2015). Discourses of cyberspace securitization in Brazil and in the United States. Revista Brasileira de Política Internacional, 58(2), p. 23–43.
152. Lundborg, T., Vaughan-Williams, N. (2011). Resilience, Critical Infrastructure, and Molecular Security: The Excess of "Life" in Biopolitics. International Political Sociology, 5(4), p. 367–383.
153. Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information Security Management Objectives and Practices: A Parsimonious Framework. Information Management & Computer Security, 16(3), p. 251–270.
154. Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An Integrated Framework for Information Security Management. Review of Business, 30(1), p. 58.
155. Manadhata, P., Wing, J. M. (2005). An Attack Aurface Metric. IEEE Transactions on Software Engineering, 37 (3), p. 371–386.
156. *McDonald M. (2008). Constructivism – Security Studies: An Introduction. Williams P. D., London: Routledge*, p. 59–72.
157. McDonald, M. (2002). Human Security and The Construction of Security. Global Society, 16(3), p. 277–295.
158. McManus, S. T. (2008). Organisational Resilience in New Zealand.

159. Mearsheimer, J. (1995). The False Promise of International Institutions. International Security, 19 (3), p.5–49.
160. Mearsheimer, J. (2013). Structural Realism – *T. Dunne, M. Kurki & S. Smith, International Relations Theory: Discipline and Diversity. Oxford: Oxford University Press*, p. 77–93.
161. Melnikov V., Kleimenov S., Petrakov A. (2008). Информационная безопасность и защита информации. Учебное пособие. *M.: Academia*. p. 44.
162. Milligan, P., Hutcheson, D. (2006). Analysis of Outsourcing and The Impact on Business Resilience. IFIP International Federation for Information Processing, 206, p. 199–208.
163. Mitchell, R. C., Marcella, R., & Baxter, G. (1999). Corporate Information Security Management. New Library World, 100(5), p. 213–227.
164. Moravcsik, A. (2001). Liberal International Relations Theory: A Social Scientific Assessment Cambridge: MA: Harvard University Press.
165. Morgan, G. (1980). Paradigms Metaphors and Puzzle Solving. Administrative Science Quarterly, 25(4).
166. Moteff, J. D. (2012). Critical Infrastructure Resilience : The Evolution of Policy and Programs and Issues for Congress. US Congressional Research Service, p. 1–20.
167. Moulton R., Coles S. R. (2003). Applying Information Security Governance. Computers & Security, 22(7).
168. Mowbray, T. J. (2013). Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions. John Wiley & Sons.
169. Nacionalinis kibernetinių incidentų valdymo planas, Nr. 87, 2016 m. sausio 25 d., Vilnius.
170. Nan C., Sansavini, G. (2017). A Quantitative Method for Assessing Resilience of Interdependent Infrastructures. Reliability Engineering and System Safety, 157, p. 35–53.
171. Nardi, B., & Kallinikos, J. (2007). Opening The Black Box of Digital Technologies: Mods in World of Warcraft.
172. Navari C. (2008). Liberalism – *Security Studies: An Introduction. Williams P. D., London: Routledge*, p. 29–43.
173. Nayak U., Rao U. (2014). The InfoSec Handbook. An Introduction to Information Security.
174. Neubauer, T., Klemen, M., Biffl, S. (2006). Secure Business Process Management: A Roadmap. Availability, Reliability and Security – *the First International Conference on, IEEE*, p. 8.
175. Neuman W. L. (2007). Basics of Social Research Qualitativeand Quanftative Approaches, 2nd Edition. Boston: Allyn & Bacon, Inc.
176. Nissenbaum, H. (2005). Where Computer Security Meets National Security. Ethics and Information Technology, 7(2), p. 61–73.
177. Nogal, M., O'Connor, A. (2017). Cyber-Transportation Resilience. Context and Methodological Framework – *Resilience and Risk. Springer, Dordrecht*, p. 415–426.

178. Nugent J. H., Raisinghani M. (2007). Bits and Bytes vs. Bullets and Bombs: A New Form of Warfare. Cyber warfare and cyber terrorism. IGI Global, p. 26–31.
179. O'Malley, P. (2010). Resilient Subjects: Uncertainty, Warfare and Liberalism, Economy and Society, 39(4), p. 488–509.
180. OECD (2004). G20/OECD Principles of Corporate Governance. OECD Publishing, Paris.
181. Peter, A. S. (2017). Cyber Resilience Preparedness of Africa's Top-12 Emerging Economies. International Journal of Critical Infrastructure Protection, 17, p. 49–59.
182. Phillips, B. (2013). Information Technology Management Practice: Impacts upon Effectiveness. Journal of Organizational and End User Computing (JOEUC), 25(4), p. 50–74.
183. Randell B., Lee P. A., Treleaven P. C. (1978). Reliability Issues in Computing System Design. ACM Computing Surveys, (10), p.123–165.
184. Ransbotham, S., and Mitra, S. (2009). Choice and Chance: A Conceptual Model of Paths to Information Security Compromise. Information Systems Research 20(1), p 121–139.
185. Reid, J. (2012). The Disastrous and Politically Debased Subject of Resilience, Development Dialogue, 58, p. 67–81.
186. Richard F., Carvalho M., Mayron L. (2012). Toward Metrics for Cyber Resilience. Diss. University of California at Davis.
187. Ridley, G. (2011). National Security as A Corporate Social Responsibility: Critical Infrastructure Resilience. Journal of Business Ethics, 103(1), p. 111–125.
188. Riolli, L., Savicki, V. (2003). Information System Organizational Resilience. Omega, 31(3), p. 227–233.
189. Risk Steering Committee. (2010). DHS Risk Lexicon: 2010 edition, p 26.
190. Rodrigues, D. D. (2014). Cyber Security vs. Information Security. Prieiga per internetą: https://www.linkedin.com/pulse/cyber-security-vs-information/.
191. Rosenthal, D. A. (2002). Intrusion Technology: Leveraging The Organization's Security Posture. Information Systems Management, 19(1), p. 3–44.
192. Rosenzweig P. (2012, May 24). The Alarming Trend of Cybersecurity Breaches and Failures in The U.S. Government. Douglas and Sarah Allison Center for Foreign Policy Studies The Heritage Foundation. Backgrounder. No. 2695. Prieiga per internetą: http://www.heritage.org/defense/report/the-alarming-trend-cybersecurity-breaches-and-failures-the-us-government.
193. Saco, D. (1999). Colonizing Cyberspace: National Security and the Internet – *Weldes, J., M. Laffey, M., Gusterson, H., Duvall R. Cultures of Insecurity: States, Communities, and the Production of Danger. Minneapolis: University of Minnesota Press*, p. 261–290.
194. Sansavini, G. (2017). Engineering Resilience in Critical Infrastructures – *Resilience and Risk. Springer, Dordrecht*, p. 189–203.
195. Schraw, G. (1998). Promoting General Metacognitive Awareness. Instructional Science, 26(1), p. 113–125.

196. Setola, R., Luiijf, E., Theocharidou, M. (2016). Critical Infrastructures, Protection and Resilience – Managing The Complexity of Critical Infrastructures, Springer International Publishing, p. 1–18.
197. Seville, E, Brunsdon, D., Dantas, A., Le Masurier, J., Wilkinson, S., Vargo, J. (2008). Organisational Resilience: Researching The Reality of New Zealand Organisations, 4(1), Journal of Business Continuity & Emergency Planning, 2 (3), p. 258–266.
198. Seville, E. (2009). Resilience: Great Concept But... What Does it Mean for Organisations? – *US Council on Competitiveness Workshop, Risk and Resilience, Wilmington, USA*, p. 9–15.
199. Shailer, 2004 Shailer, G. E. (2004). Introduction to Corporate Governance in Australia. Pearson Education Australia.
200. Shamir, A. Cryptography: State of Science. Turing Award Lecture 2002. Prieiga per internetą: http://amturing.acm.org/vp/shamir_0028491.cfm.
201. Shapiro, S. (2016). A Framework for Assessing Cyber Resilience. A Report for The World Economic Forum. Prieiga per internetą: http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf
202. Sherwood, J. Clark, A. Lynas, D. (2005). Enterprise Security Architecture: A Business-Driven Approach. CRC Press.
203. Silic M., Back A. (2014). Information Security: Critical Review and Future Directions for Research., Information Management & Computer Security, 22(3), p. 279–308.
204. Singer P.W., Friedman A. (2013). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press.
205. Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. Global Journal of Flexible Systems Management, 14(4), p. 225–239.
206. Siponen, M. T. (2000). A Conceptual Foundation for Organizational Information Security Awareness. Information Management & Computer Security, 8(1), p. 31–41.
207. Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study. Information & Management, 51(2), p. 217–224.
208. Siponen, M., Willison, R. (2009). Information Security Management Standards: Problems and Solutions. Information & Management, 46(5), p. 267–270.
209. Solms S.H. Solms R. (2009). Information Security Governance. Springer Science Business Media, LLC.
210. 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(2), p. 215–225.
211. Spirtas, M. (1996). A House Divided: Tragedy and Evil in Realist Theory. Security Studies, 5(3), p. 385–423.
212. Stahl B.C., Shaw M., Doherty N. (2008, December 13). Information Systems Security Management: A Critical Research Agenda. *Association of Information Systems SIGSEC Workshop on Information Security & Privacy*, Paris.

213. Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of End User Security Behaviors. Computers & Security, 24(2), p. 124–133.
214. Starr, R., Newfrock, J., Delurey, M. (2003). Enterprise Resilience: Managing Risk in The Networked Economy. Strategy and Business, (30), p. 70–79.
215. Steinbart, P. J., Raschke, R. L., Gal, G., Dilla, W. N. (2012). The Relationship Between Internal Audit and Information Security: An Exploratory Investigation. International Journal of Accounting Information Systems.
216. Stephenson, A., Vargo, J., & Seville, E. (2010). Measuring and comparing organisational resilience in Auckland. *Australian Journal of Emergency Management, The*, *25*(2), 27.
217. Straub, D.W. Welke, R. J. (1998). Coping With Systems Risks: Security Planning Models for Management Decision Making. MIS Quarterly, 22, p. 441–469.
218. Strens, R. & Dobson, J. (1993). How Responsibility Modeling Leads to Security Requirements. Proceedings of The 16th National Computer Security Conference, Baltimore, MD, p. 398–408.
219. Sutcliffe K. M. Vogus J. (2003). Organizing for Resilience Positive Organizational Scholarship. Foundations of A New Discipline. K. S. Cameron, J. E. Dutton and R. E. Quinn. San Francisco, CA, Berrett-Koehler, p. 94–110.
220. Szefer, J., Keller, E., Lee, R. B., Rexford, J. (2011). Eliminating The Hypervisor Attack Surface for A More Secure Cloud CCS'11, p. 17–21.
221. Tassey G. (1999). Standardization in Technology-Based Markets. Research Policy 29 (4-5), p. 587–602.
222. Thebeau, D., Reidy, B., Valerdi, R., Gudagi, A., Kurra, H., Al-Nashif, Y., Sheldon, F. (2014). Improving Cyber Resiliency of Cloud Application Services by Applying Software Behavior Encryption (SBE). Procedia Computer Science, 28(Cser), p. 62–70.
223. Tierney K., Bruneau M. (2007, May). Conceptualizing and Measuring Resilience A Key to Disaster Loss Reduction. TR News 250. The National Academies of Sciences, Engineering, and Medicine.
224. Tierney, K. J. (2003). Conceptualizing and Measuring Organizational and Community Resilience: Lessons from The Emergency Response Following the September 11, 2001 Attack on the World Trade Center.
225. Tipton, H. F., & Nozaki, M. K. (2007). Information security management handbook. CRC press.
226. Todorovic, B., Trifunovic, D., Jonev, K., Filipovic, M. (2017). Contribution to Enhancement of Critical Infrastructure Resilience in Serbia – *Resilience and Risk. Springer, Dordrecht,* p. 531–551.
227. Tran, H., Campos-Nanez, E., Fomin, P., Wasek, J. (2016). Cyber Resilience Recovery Model to Combat Zero-Day Malware Attacks. Computers and Security, 61, p. 19–31.
228. Trucco, P., Petrenj, B. (2017). Resilience of Critical Infrastructures: Benefits and Challenges from Emerging Practices and Programmes at Local Level – *Resilience and Risk. Springer, Dordrecht*, p. 225–286.

229. Trump, B. D., Poinsatte-Jones, K., Elran, M., Allen, C., Srdjevic, B., Merad, M., Palma-Oliveira, J. M. (2017). Social Resilience and Critical Infrastructure Systems – *Resilience and Risk. Springer, Dordrecht*. p. 289–299.
230. Tseng, P. T., Yen, D. C., Hung, Y. C., & Wang, N. C. (2008). To Explore Managerial Issues and Their Implications on e-Government Deployment in the Public Sector: Lessons from Taiwan's Bureau of Foreign Trade. Government Information Quarterly, 25(4), p. 734–756.
231. U.S. Joint Chiefs of Staff (2012). Joint Publication 3–13. Information Operations. Prieiga per internetą: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.
232. Uddin M., Memon J., Alsaqour R., Shah A., Rozan M.Z.A. (2015). Mobile Agent Based Multi-layer Security Framework for Cloud Data Centers. Indian Journal of Science and Technology, 8(12).
233. Ullman, R. H. (1983). Redefining Security. International Security, 8(1), p. 129–153.
234. Urciuoli, L. (2015). Cyber-Resilience: A Strategic Approach for Supply Chain Management. Technology Innovation Management Review, 5(4), p. 13–19.
235. Vogus, T. J., & Sutcliffe, K. M. (2007, October). Organizational Resilience: Towards A Theory and Research Agenda. In Systems, Man and Cybernetics, 2007. ISIC. *IEEE International Conference on IEEE*, p. 3418–3422.
236. Von Solms, B., & Von Solms, R. (2005). From Information Security to ... Business Security? Computers & Security, 24(4), p. 271–273.
237. Von Solms, R., & Van Niekerk, J. (2013). From Information Security to Cyber Security. Computers & Security, 38, p. 97–102.
238. Von Solms, S. H., & Von Solms, R. (2009). In Information Security Governance. Springer, Boston, MA.
239. Vugrin, E. D., Turgeon, J. (2013). Advancing Cyber Resilience Analysis with Performance-Based Metrics from Infrastructure Assessments. International Journal of Secure Software Engineering, 4(1), p. 75–96.
240. Wæver, O. (1995). Securitization and Desecuritization – *R. D. Lipschutz (Ed.). On Security. Columbia University Press*, p. 46–87.
241. Wæver, O. (2011). Politics, Security, Theory. Security Dialogue, 42(4–5), p. 465–480.
242. Walker, J., Cooper, M. (2011). Genealogies of Resilience: From Systems Ecology to The Political Economy of Crisis Adaptation. Security Dialogue, 14(2), p. 143–160.
243. Wang, J. W., Gao, F., Ip, W. H. (2010). Measurement of Resilience and Its Application to Enterprise Information Systems. Enterprise Information Systems, 4(2), p. 215–223.
244. Welch, E. W., & Pandey, S. K. (2006). E-Government and Bureaucracy: Towards a Better Understanding of Intranet Implementation and Its Effect on Red Tape. Journal of Public Administration Research and Theory, 17(3), p. 379–404.
245. Welsh M. (2014). Resilience and Responsibility: Governing Uncertainty in A Complex Eorld. The Geographical Journal, 180 (1), p. 15–26.

246. Werfs, M., & Baxter, G. (2013). Towards Resilient Adaptive Socio-Technical Systems – *Proceedings of the 31st European Conference on Cognitive Ergonomics – ECCE'13*, p. 1–4.
247. White G. B. (2007). The Community Cyber Security Maturity Model – *Proceedings of the 40th Hawaii International Conference on System Sciences*.
248. White, G. (2009). Strategic, Tactical, & Operational Management Security Model. Journal of Computer Information Systems, 49(3), p. 71–75.
249. Whitman, M. E., & Mattord, H. J. (2012). Principles of InformationSsecurity. Cengage Learning.
250. Wilding, N. (2016). Cyber Resilience: How Important is Your Reputation? How Effective Are Your People? Business Information Review, 33(2), p. 94–99.
251. Willcocks, L. Margetts, H. (1994). Risk Assessment and Information Systems. European Journal of Information Systems, 3, p. 127–139.
252. Williams A. H., Manheke, R. J. (2010). Small Business – A Cyber Resilience Vulnerability, (August) – *Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 2010, August 23*.
253. Williams P. D. (2008). Security Studies: An Introduction. London: Routledge.
254. Williams, P. A. H. (2010). Is Cyber Resilience in Medical Practice Security Achievable? – *Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 2010, August 23*.
255. Willison, R., & Siponen, M. (2007, January). A Critical Assessment of IS Security Research Between 1990–2004 – *Proceedings of 15th European Conference on ISs, St. Gallen, Switzerland*, p. 1551–1559.
256. Woods, D. D., & Wreathall, J. (2008). Stress-Strain Plots as A Basis for Assessing System Resilience. *R*esilience engineering: Remaining sensitive to the possibility of failure, 1, p. 145–161.
257. Z/Yen Group (2015). Promoting UK Cyber Prosperity: Public-Private Cyber-Catastrophe Reinsurance. A Long Finance report prepared by Z/Yen Group Co-sponsored by APM Group.
258. Zacher, M., Matthew R. (1995). Liberal International Theory: Common Threads, Divergent Strands' in Charles Negley (ed.), Controversies in International Relations Theory. New York: St Martin's Press, p. 107–150.
259. Zafar, H., & Clark, J. G. (2009). Current State of Information Security Research in IS. Communications of the Association for Information Systems, 24(1), p. 34.
260. Zissis, D., and Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture. Government Information Quarterly, 28(2), p. 239–251.
261. Zussblatt, N. P., Ganin, A. A., Larkin, S., Fiondella, L., Linkov, I. (2017). Resilience and Fault Tolerance in Electrical Engineering – *Resilience and Risk. Springer, Dordrecht*, p. 427–447.

PRIEDAI

1 PRIEDAS

Organizacinio atsparumo modeliai

Pavadinimas	Apibūdinimas
Integruotas - funkcinis	**Modelio esmė:**
	Atsparumas integruojamas į jau egzistuojančius teorinius instrumentus: veiklos tęstinumo ar nenumatytų situacijų, rizikų bei kokybės valdymą.
	Trūkumai:
	Ankstyvieji organizacinio atsparumo konceptai, ypač JK ir JAV, buvo pagrįsti įvairių senai egzistuojančių veiklos tęstinumo valdymo požiūrių nauju pateikimu, įvardijant juos atsparumo procesais arba atsparumo sistemomis, kurios buvo matomos kaip galinčios turėti tokį patį efektą atsparumui, kokį turėjo IS09001 standartas kokybės valdymui. Pagal autorius, toks norminis požiūris ne tik kelia riziką netinkamo atsparumo suvokimo formavimuisi, bet ir kelia grėsmę jau suformuoto atsparumo lygmens sumažinimui, ypač ekstremalių, nenumatytų ir neprognozuotų įvykių akivaizdoje. Anot autorių, toks požiūris iki galo nepaaiškina atsparumo (Gibson, Tarrant, 2011).
	Privalumai:
	Nepaisant trūkumų, nereiškia, kad tokie požiūriai iš esmės yra netinkami, procesų valdymu pagrįstas sisteminis mąstymas turi gana nemažai skirtingo profilio sėkmingai įgyvendintų pavyzdžių. Integruojant atsparumą su rizikų valdymo programomis, galima pastebėti pakankamai ženklų indėlį į organizacinį atsparumą. Integruojant atsparumą į tam tikrą egzistuojantį modelį, pavyzdžiui, rizikų valdymo, atsparumui suformuojamas tam tikras pagrindas, kuris suformuoja sąsajas tarp skirtingų organizacinių gebėjimų, tokių kaip nenumatytų situacijų, veiklos tęstinumo, saugos ir krizių valdymas. Pats rizikų valdymas naudingas atsparumo formavimui ir tuo, kad padeda suformuoti bendrą suvokimą apie tai, kaip iš didelį nežinomumo laipsnį turinčių aplinkų kylančios rizikos gali paveikti organizacijos tikslus bei pateikti specializuotais gebėjimais pagrįstą priemonių rinkinį šiems nežinomiems iššūkiams spręsti (Gibson, Tarrant, 2011).
Pavadinimas	**Apibūdinimas**
Atribucinis	**Modelio esmė:**
	Atsparumas bandomas paaiškinti iš didelį atsparumą turinčių organizacijų perspektyvos. Toks požiūris padeda atskleisti, kokie organizaciniai atributai gali padėti organizacijai atsakyti į nežinomybės ir nenumatytų situacijų keliamus iššūkius. Taigi, atribuciniai modeliai gali pateikti duomenų apie tai, kokius pokyčius organizacija turėtų įgyvendinti siekdama pagerinti savo atsparumo būklę. Atribuciniame modelyje turėtų būti akcentuojami du esminiai faktoriai: Organizacinės vertybės – įsipareigojimų, pasitikėjimo ir stipraus vidinio suderinimo bei bendros prasmės formavimas; Lyderystė – aiškių strateginių krypčių formavimas remiantis rizikų suvokimu ir kitų įgalinimas įgyvendinti strateginę viziją, pasitikėjimo skiepijimas.
	Trūkumai:
	Nepakankamai įvertinami „kietieji“ (angl. *hard*) organizacijos elementai, nepaaiškina atsparumo.

	Privalumai:
	Vertybės ir lyderystė ilgainiui sukuria organizacinę kultūrą ir gebėjimus, kurie padeda žinoti, suprasti ir išsiugdyti tam tikrą jautrumo laipsnį vidiniams ir išoriniams pokyčiams. Pagal Gibson ir Tarrant (2011), šiame kontekste aktualiomis tampa Peche ir Oakley (2005) idėjos, apimančios aukšto lygio pokyčių jautrumą ir įžvalgumą per praėjusių įvykių suvokimą, dabarties stebėseną ir situacijos žinojimą (angl. *situational awareness*) – toks tinkamas praeities ir dabarties įvertinimas kartu su tinkama komunikacija ugdo gebėjimą prognozuoti ateitį ir taip leidžia identifikuoti esminių galimų pokyčių indikatorių. Visi šie faktoriai lemia didesnę atskirų organizacijos dalių integraciją, sudarydami sąlygą geresnei jų kooperacijai esant nenumatytiems įvykiams. Šių įvairių elementų operavimas užtikrinamas per atvirą, adekvačią komunikaciją, kuri suformuoja bendrą padėties suvokimą ir sukuria organizacijai kylančių rizikų dinamikos žinojimo būseną. Visų šių elementų balansavimas sukuria organizacinį judumą (angl. *agility*), kuris reikalingas organizacijai atsakyti į nenuspėjamos aplinkos keliamus iššūkius. Tokio pobūdžio atribuciniai modeliai gali būti ypač naudingi koncentruojantis ties ir bandant suprasti „minkštuosius“ (angl. *soft*) atsparumo aspektus (Gibson ir Tarrant, 2011).
Pavadinimas	**Apibūdinimas**
Kompozitinis	**Modelio esmė:**
	Priešingai net Atribucinis, Kompozitinis modelis apima abi grupes, t.y. „minkštųjų“ ir „kietųjų“ (angl. *soft and hard*) elementų operacijas: procesus, infrastruktūrą, technologijas, resursus, informaciją ir žinias. Modelio pagrindą sudaro orientacija į strategijas ir politikas, formuojančias operacijų dualumą (angl. *duality*), gebėjimus operuoti ir rutininėse, ir nerutininėse aplinkose. Pagal Gibson ir Tarrant (2011), šiame modelyje labai svarbų vaidmenį užima kylančios lyderystės vaidmuo, išreiškiamas Norhouse (2000) ir Mintzburg (1985) idėjomis siekiant sąlygoti kitų organizacijos elementų pokyčius ir jų prisiderinimą prie nerutininių aplinkų.
	Trūkumai:
	Gali būti sudėtingiau diegiamas technologinėse organizacijose, kaip ir Integruotojo modelio atveju – nepaaiškina atsparumo Gibson ir Tarrant (2011).
	Privalumai:
	Kylanti lyderystė yra matoma kaip galinti suformuoti pagerinta nenuspėjamumo suvokimą bei pakankamai operatyviai galinti šį suvokimą transformuoti į reikiamus sprendimus ir veiksmus. Taip suformuojamos veiklos kryptys esant dideliems neužtikrintumo ir dviprasmiškumo momentais siekiant pritaikyti atsparumo gebėjimus ir unifikuojant procesus, resursus, infrastruktūrą, technologijas, informacijas ir žinias. Svarbu pažymėti, kad lyderystė nebūtinai kyla iš aukščiausios grandies vadovybės, bet dažniausiai talentingi vidutinio lygmens vadybininkai yra ta terpė, kurioje pradedamos atsparumo komponentų lyderystės integracija Gibson ir Tarrant (2011).
Pavadinimas	**Apibūdinimas**
	Modelio esmė:
	Bandomi apjungti keliuose modeliuose esantys atsparumo konceptai, taip užpildant kiekviename jų egzistuojančias spragas.

Eglės šablono (Herringbone)	Modelyje pripažįstama, kad pagal nutylėjimą, dauguma organizacijų pastaruoju metu jau turi reikšmingus gebėjimus ir imasi aibės veiksmų, galinčių pagerinti atsparumo lygį. Be to, organizacijos demonstruoja aibę charakteristikų, kurios paveikia gebėjimų, leidžiančių padidinti organizacijos atsparumą. Nors dauguma šių gebėjimų apima organizacijų veiklas ir charakteristikas, kurios yra kritinės rutininėse aplinkose, būtent jų gebėjimai adaptuoti šiuos gebėjimus nerutininėms aplinkoms formuoja atsparumą. Kai kurie gebėjimai ir veiklos yra savo prigimtimi specifiškos ir aktualios veikimui nerutininėse aplinkose. Tai apima tokius elementus, kaip veiklos tęstinumas bei nenumatytų situacijų ir krizių valdymas. Tačiau tam tikros charakteristikos yra nepriklausomos nuo bendros veiklų nenumatytose situacijose aibės, tačiau padeda suformuoti atsparumą per geresnį operavimą tokiose nerutininėse aplinkose. Šių charakteristikų svarba priklauso nuo kintančių aplinkybių, su kuriomis konkrečiu metu susiduria organizacija, prigimties. Pagal Gibson Tarrant (2011) šios savybės yra: regumas (angl. *acuity*) – gebėjimas prioretizuoti įvykius, kurie buvo praeityje; situacinis žinomumas (angl. *situational awareness*) – mokėjimas nustatyti dabartinę situaciją ir; įžvalgos (angl. *foresight*) – suvokimas, kas galėtų įvykti ateityje. Regumas suteikia gebėjimą surinkti informaciją ir identifikuoti ankstyvus perspėjimo indikatorius, susijusius su dramatišku pokyčiu ir pateikia kelis galimus reagavimo į jį būdus. Tolerancija dviprasmiškumui (angl. *ambiguity tolerance*) – gebėjimas priimti sprendimus ir imtis veiksmų esant dideliam neužtikrintumo laikui. Kreatyvumas ir judumas (angl. *creativity and agility*) – operavimas pasitelkiant inovatyvius metodus siekiant rasti problemos sprendimo būdus, tokiu greičiu, kuris atitiktų neapibrėžtumo keliamus iššūkius. Susidorojimas su stresu (angl. *stress coping*) – žmonių, procesų ir infrastruktūros gebėjimas operuoti esant padidintiems reikalavimams ir nežinomumo lygiui. Mokymosi gebėjimai (angl. *learnability*) – gebėjimai apimantys organizacijos sugebėjimą mokytis iš savo ir kitų patirčių, gebėjimas geriau valdyti vyraujančias patirtis ir mokytis iš realiu laiku vykstančių pamokų. Svarbi modelio dalis yra ir veiklos bei gebėjimai, kurie apima: valdyseną, sprendimų priėmimą, *suinteresuotuojų pusių* gebėjimus, atitikties (angl. *compliance*), rizikų valdymą, komunikaciją, žmogiškuosius gebėjimus, veiklos tęstinumo ir krizių valdymą, infrastruktūros ir technologijų gebėjimus, nepaprastų situacijų valdymą, santykių (angl. *relationship*) valdymą, resursų gebėjimus, finansinį valdymą. Lyderystę, strateginį tikrumą (angl. *strategic surety*), organizacijos kultūrą, streso valdymą, vertybes, elgseną, mokymosi gebėjimus, pasitikėjimą, judumą (angl. *agility*), kreatyvumą, vidines organizacijos jungtis (angl. *interconnections*), neapibrėžtumo toleranciją (Gibson ir Tarrant, 2011).
	Trūkumai:
	Pernelyg kompleksiškas ir sudėtingas, apimantis daug organizacijos sisteminių elementų, nepaaiškina atsparumo.
	Privalumai:
	Išsamus, apimantis daug organizacijos sričių, sąlygojančių atsparumo susiformavimą.
Pavadinimas	**Apibūdinimas**

Atsparumo trikampio	**Modelio esmė:**
	Sudaro į tris kategorijas konceptualiai paskirstyti komponentai: procesiniai, resursiniai ir infrastruktūriniai gebėjimai bei lyderystės, žmogiškųjų resursų, žinių gebėjimai. Akcentuoja kiekvienos atsparumo srities lakią (angl. *fluid*) prigimtį. Toks kiekvieno elemento lakumas kyla iš organizacinių procesų, kurie nuolatos peržiūri, įvertina ir adaptuoja savo gebėjimus kiekvienoje trikampio pusėje: Yra tinkami naudoti pagal paskirtį (angl. *fit for purpose*) – jų dizaino parametrai atitinka reikiamų atlikti uždavinių keliamus reikalavimus, šios veiklos reikalauja atidžios gebėjimų ir kintamumo laipsnio stebėsenos bei šių dviejų reiškinių tarpusavio adekvatumo palyginimo. Tinkamų pajėgumų išlaikymas, siekiant įsitikinti, kad būtini organizaciniai tikslai bus pasiekti – tai dažnai reikalauja, kad šių gebėjimų dizainas būtų gebantis atsispirti arba tolerantiškas stresui. Demonstruoja lankstumą praplėsti atsparumą už pradinių dizaino parametrų ribų, besikeičiant aplinkybėms. Atsparumo trikampio diagramą sudaro iš keturių kvadrantų sudarytas centrinis apskritimas, apimantis: lankstumą, gebėjimus ir sistemos tvirtumą. Pats apskritimas konceptualiai pozicionuojamas iš trijų sektorių sudaryto trikampio, kuris pats yra supamas kontekstų, kurie veikiami atsparumo. Taigi, bet koks vieno ar kelių gebėjimų efektyvumo praradimas sumažina atsparumą. Kiekvienas vykstantis atsparumo gebėjimų praplėtimas, sumažėjimas ar patobulinimas priklauso nuo gebėjimų sąveikos prigimties kiekviename specifiniame vidiniame ar išoriniame kontekste (Gibson, Tarrant, 2011).
	Trūkumai:
	Modelio kūrėjai pažymi, kad viena trikampio kategorija priklauso nuo kitos, tad modelis gali būti įgyvendinamas tik pilnai, negalimas fragmentinis diegimas, ar diegimas iteracijomis (Gibson ir Tarrant, 2010).
	Privalumai:
	Išskirti esminiai, vienas nuo kito priklausomi komponentai, kurie yra esminiai organizaciniam atsparumui formuoti (Gibson, Tarrant, 2010).

Šaltinis: *Gibson ir Tarrant (2010)*

2 PRIEDAS

Dalyvio sutikimo forma
Dalyvio sutikimas

Aš, _____, esu informuota (-as), kad:

1. Interviu duomenys bus naudojami Mykolo Romerio universiteto vadybos mokslo krypties valstybės nefinansuojamų ištęstinių doktorantūros studijų studento Roko Grincevičiaus disertacijoje tema „Kibernetinio saugumo valdymo gerinimas taikant atsparumo modelius organizacijose“.
2. Sutinku, kad:

- ☐ apdorojant duomenis asmeninė respondento informacija (vardas ir pavardė) būtų skelbiami;
- ☐ apdorojant duomenis asmeninė respondento informacija (vardas ir pavardė) būtų užkoduoti ir neskelbiami;
- ☐ apdorojant duomenis asmeninė respondento informacija (institucija) būtų skelbiama;
- ☐ apdorojant duomenis asmeninė respondento informacija (institucija) būtų užkoduota ir neskelbiama;
- ☐ apdorojant duomenis asmeninė respondento informacija (pareigos) būtų skelbiama;
- ☐ apdorojant duomenis asmeninė respondento informacija (pareigos) būtų užkoduota ir neskelbiama.

3. Interviu tikslas yra identifkuoti kibernetinio atsparumo didinimo galimybes viešojo sektoriaus organizacijose. Interviu metu pateikiami klausimai, apimantys 8 temas: Kibernetinio atsparumo etoso formavimas organizacijoje, atsparumo pozicionavimas; Kibernetinio saugumo situacijos žinomumo gerinimas; Esminių pažeidžiamumų valdymas; Adaptyvių gebėjimų valdymas; Sistemos lankstumo gerinimas; Reakcijos į kibernetines atakas gerinimas; Kibernetinių atakų paviršiaus sumažinimas; Rizikų valdymas. Numatoma interviu trukmė – apie 1 val.
4. Dalyvavimas tyrime yra neatlygintinas.
5. Tyrimo rezultatai bus publikuojami viešai, respondentų asmeniniai duomenys bus skelbiami / neskelbiami vadovaujantis respondento sutikimu dėl asmeninių duomenų.
6. Iškilus klausimams, susijusiems su tyrimu arba dalyvavimu jame, galima kreiptis į Roką Grincevičių, Mykolo Romerio universitetas, Vilnius, Lietuva, tel. +370 60737499, el. pašto adresas: rokas.grincevicius@gmail.com.

Aš susipažinau su aukščiau pateikta informacija. Aš suprantu, kad bet kuriuo metu galiu atsisakyti dalyvauti interviu. Šio sutikimo kopija man yra pasiūlyta.

_____

Tyrimo dalyvio parašas, vardas ir pavardė

_____

Data

_____

Kontaktinis telefonas, el. paštas

3 PRIEDAS

Kibernetinio atsparumo matrica

Dimensija / domenas	Planavimas ir pasirengimas	Detektavimas	Absorbavimas	Atsistatymas	Adaptacija
Fizinė	1. Kritinių vertybių kontrolės sensorių diegimas. 2. Kritinių paslaugų kontrolės sensorių diegimas. 3. Tinklų struktūros ir jų sisteminių jungčių komponentų įvertinimas. 4. Kritinės fizinės infrastruktūros dubliavimas. 5. Logiškai ar fiziškai nuo tinklo atskirtų duomenų dubliavimas.	1. Fizinės aplinkos stebėsena, siekiant nustatyti potencialius kibernetinio saugumo įvykius. 2. Personalo veiklos stebėsena siekiant nustatyti potencialius kibernetinius įvykius.	1. Vertybių ar servisų grėsmių signalizavimas. 2. Atliekamų vertybių paslaugų tęstinumui naudojimas. 3. Resursų, apsiginti nuo atakų dedikavimas.	1. Neveikiančių kontrolės sensorių nustatymas ir sutvarkymas. 2. Paslaugoms / vertybėms padarytos žalos įvertinimas. 3. Funkciniam atsistatymui reikalingo laiko įvertinimas. 4. Nesutaisomų vertybių saugi utilizacija.	1. Konfigūracijos peržiūra ir pertvarkymas, atsižvelgiant į paskutiniuosius įvykius. 2. Palaipsninis sugadintų vertybių naudojimo nutraukimas, naujų vertybių naudojimo pradėjimas.
Informacinė	1. Fizinių įrenginių, sistemų, programinės įrangos inventorizacija. 2. Organizacijos komunikacijos ir duomenų srautų žemelapiavimas. 3. Išorinių sistemų katalogavimas. 4. Vertybių kategorizavimas, remiantis kritiškumu ar atsparumo reikalavimais. 5. Kritinių sistemų rangovų dokumentavimas pagal jų turimą kvalifikaciją.	1. Užkrėsto kodo detektavimas. 2. Neautorizuotos prieigos detektavimas. 3. Išorinių paslaugų teikėjų stebėsena, siekiant identifikuoti potencialius kibernetinio saugumo įvykius.	1. Kritinių paslaugų ir vertybių sensorių stebėjimas. 2. Efektyvus atitinkamos informacijos ir duomenų teikimas atsakingiems sprendimų priėmėjams ir suinteresuotoms šalims.	1. Sensorių ir įvykių žurnalinės informacijos rinkimas įvykio metu. 2. Sistemų palyginimas prieš ir po įvykio.	1. Incidentų poveikio ir priežasčių dokumentavimas. 2. Laiko tarp problemos nustatymo ir atsistatymo dokumentavimas. 3. Ateities sistemos būsenų numatymas po atsistatymo. 4. Atakos, įsilaužimo taškų dokumentavimas.

	6. Klasifikuotos ir jautrios informacijos saugojimo planų ir tvarkų parengimas. 7. Išorinių priklausomybių identifikavimas. 8. Vidinių priklausomybių identifikavimas.		5. Audito žurnalinių įrašų dokumentavimas diegimas bei peržiūra, atsižvelgiant į egzistuojančias saugos politikas ir procedūras.		5. Incidentų kategorizavimas pagal atsako planus. 6. Nuolatinis apsaugos procesų tobulinimas.
Kognityvinė	1. Įvykių ir sistemų būsenos pasikeitimų numatymas, planavimas. 2. Našumo kompromisų suvokimas organizacijos tikslų siekime. 3. Scenarijais pagrįstas kibernetinio karo imitavimas (angl. wargaming). 4. Kibernetinio saugumo įtraukimas į žmogiškųjų resursų valdymo praktikas. 5. Testavimo, atsako ir atsistatymo planai.	1. Detektuotų įvykių analizė siekiant suprasti atakų taikinius ir metodus. 2. Įvairių šaltinių ir sensorių įvykių duomenų agregavimas ir koreliacija. 3. Įvykių poveikio nustatymas. 4. Incidentų perspėjimo mechanizmų apatinių ribų nustatymas.	1. Sprendimų priėmimo protokolų ar pagalbinių priemonių naudojimas, siekiant nustatyti, kad įvykis yra vykstantis. 2. Gebėjimo įvertinti poveikį sistemos našumui, siekiant nustatyti ar įmanoma tęsti misiją, formavimas. 3. Susitelkimo ties identifikuotomis kritinėmis vertybėmis ir paslaugomis didinimas. 4. Tinkamų planų sistemų būsenoms, kuomet tai yra įmanoma, naudojimas.	1. Kritinių techninių ir informacijos aspektų peržiūra, siekiant priimti informuotus sprendimus. 2. Sprendimų priėmimo protokolų ir atsistatymo pasirinkimo priemoniųnustatymas.	1. Vadovaujančios grandies atsako ir sprendimų priėmimo procesų peržiūra. 2. Atakos motyvų nustatymas. 3. Naujai atrastų pažeidžiamumų sumažinimas ar jų dokumentavimas žinomais pažeidimais. 4. Incidentų poveikio suvokimas.

Socialinė	1. Koordinacija su identifikuotomis išorinėmis suinteresuotomis šalimis, galinčiomis būti paveiktomis kibernetinių atakų. 2. Darbuotojų mokymai apie atsparumą ir atsparumo planavimą. 3. Vartotojų ir autorizuotos įrangos identifikacijos priemonių valdymas. 4. Išorinės prieigos prie vertybių prieigos kontrolė ir apsauga. 5. Atsparumo komunikacijos parengimas ir formavimas. 6. Kibernetinio žinojimo kultūros formavimas. 7. Teisinių kibernetinio atsparumo reikalavimų supratimas, valdymas, apimantis privatumą, pilietines laisves ir pareigas.	1. Rolių ir atsakomybių nustatymas siekiant nustatyti detektavimo atskaitomybę. 2. Detektavimo informacijos komunikacija suinteresuotoms šalims. 3. Nuolatinis detektacijos priemonių gerinimas.	1. Atsakingų darbuotojų ir atsparumo ekspertų suradimas ir identifikavimas. 2. Komunikacijos ir kontrolės tinklų apsaugojimas. 3. Apsauginių technologijų efektyvumo aspektų pasidalinimas su suinteresuotomis šalimis.	1. Viešųjų ryšių valdymas ir reputacijos atstatymas po įvykių. 2. Atsistatymo veiklų komunikavimas vidinėms suinteresuotoms šalims ir vykdančiosios valdžios komandoms. 3. Atsakomybių nustatymas organizacijoje.	1. Darbuotojų pasirengimo įvykiams įvertinimas, siekiant nustatyti pasirengimo ir komunikacijos efektyvumą. 2. Darbuotojų priskyrimas toms sritims, kurios anksčiau nebuvo pakankamai įvertintos. 3. Informacijos rinkimas apie vėliausias grėsmes bei tendencijas apie egzistuojančius apsaugos metodus, dalintis šia informacija organizacijoje. 4. Savanoriškas dalinimasis informacija su išorinėmis suinteresuotomis šalimis, kad pasiekti didesnį kibernetinio saugumo situacijos žinomumą.

Šaltinis: *Shapiro (2016)*

MYKOLO ROMERIO UNIVERSITETAS

Rokas Grincevičius

KIBERNETINIO SAUGUMO VALDYMO GERINIMAS TAIKANT ATSPARUMO MODELIUS ORGANIZACIJOSE

Daktaro disertacija
Socialiniai mokslai, vadyba (03 S)

Vilnius, 2019

Mokslo daktaro disertacija rengta 2012–2018 metais Mykolo Romerio universitete pagal Vytauto Didžiojo universitetui su Klaipėdos universitetu, Aleksandro Stulginskio universitetu, Mykolo Romerio universitetu ir Šiaulių universitetu Lietuvos Respublikos švietimo ir mokslo ministro 2011 m. birželio 8 d. įsakymu Nr. V-1019 suteiktą doktorantūros teisę.

Mokslinė vadovė: prof. dr. Aelita Skaržauskienė (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, 03 S)

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

Pirmininkas:
prof. dr. Tadas Limba (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, 03S)

Nariai:
prof. dr. Audrius Gargasas (Vytauto Didžiojo universitetas, socialiniai mokslai, vadyba, 03S);
prof. dr. Sandro Gerić (Zagrebo universitetas, Kroatija, technologijos mokslai, informatikos inžinerija, 07T);
prof. dr. Diana Šaparnienė (Šiaulių universitetas, socialiniai mokslai, vadyba, 03S);
prof. dr. Darius Štitilis (Mykolo Romerio universitetas, socialiniai mokslai, teisė, 01S).

Daktaro disertacija bus ginama viešame Vadybos mokslo krypties tarybos posėdyje 2019 m. balandžio 12 d. 10 val. Mykolo Romerio universitete, I-414 auditorijoje.
Adresas: Ateities g. 20, 08303, Vilnius, Lietuva.

Daktaro disertacijos santrauka išsiųsta 2019 m. kovo 12 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), Šiaulių universiteto (Vytauto g. 84, Šiauliai), Vytauto Didžiojo universiteto (K. Donelaičio g. 52, Kaunas) bibliotekose.

ĮVADAS

Temos aktualumas. Įvairioms žmogiškoms veikloms persikeliant į elektroninę erdvę, taip pat vyksta ir tradicinio bei kibernetinio nusikalstamumo konvergencija, pašalinanti visas egzistuojančias ribas tarp fiziniais metodais vykdomų nusikalstamų veikų ir virtualių nusikaltimų. Atsiradus naujiems veiklos modeliams, nusikaltėliai atranda ir naujus nusikaltimo būdus, kuriuose elektroninės priemonės ir duomenys gali būti taikiniu arba atliekamo nusikaltimo įrankiu. Nusikaltimų, teroristinių išpuolių, pramoninio ir politinio šnipinėjimo vykdymo atvejų prieš fizinius asmenis, organizacijas, valstybes, kritinę infrastruktūrą kasmet vis daugėja. 2017 m. birželį įvykdyta didžiulio masto kibernetinė ataka nukreipta prieš verslo įmones, oro uostus, bankus ir valstybines institucijas Ukrainoje[35], kuri vėliau išplito ir kitose Europos valstybėse, tarp jų ir Lietuvoje. Tai buvo antroji ataka, po vos tik prieš kelias savaites įvykusios ir 150 valstybių paveikusios WannaCry atakos - nukreiptos ne tik prieš pavienes organizacijas, bet ir tokias svarbias funkcijas atliekančias sistemas, kaip Jungtinės Karalystės Nacionalinės sveikatos tarnyba. Jungtinės Karalystės gynybos sekretorius seras Michael Fallon netgi įspėjo už atakas atsakingą šalį, kad į ateities kibernetines atakas Jungtinė Karalystė galėtų atsakyti karinių oro pajėgų smūgiais ar netgi prieš jų rengėjus pasiųsti kariuomenę. Pasak sekretoriaus, tokie kibernetiniai išpuoliai „galėtų iššaukti atsaką iš bet kurio domeno – oro, žemės, jūros ar kibernetinės erdvės“[36]. Kibernetinės grėsmės reikalauja vis didesnių resursų naujų, adekvačių atsako formų paieškoms, sąlygoja sisteminius veiklos sutrikdymus ir milžiniškus finansinius nuostolius. Pagal Jungtinės Karalystės draudimo rinkos Lloyd's of London vertinimą, kibernetinės atakos verslui globaliai per vienerius metus kainuoja 400 milijardų JAV dolerių (Hubbard, Seiersen, 2016). Globali draudimo bendrovė XL Catlin, savo draudimo produktų linijoje siūlančioje ir galimybę apsidrausti nuo kibernetinių incidentų sukeltų nuostolių, kibernetines grėsmes įvardino didžiausiomis sisteminėmis grėsmėmis, kurias ji matė per visa savo daugiau nei 40 metų trunkančią praktiką draudimo versle (Z/Yen Group, 2015). Kibernetinės priemonės taip pat vis dažniau tampa geopolitinio konflikto instrumentu naujai besiformuojančių nekonvencinių priešpriešos formų kontekste. Kaip pažymi Rusijos generalinio štabo generolas Valerijus Gerasimovas, XXI a. karai daugiau nėra skelbiami, o blunkant riboms tarp karo ir taikos būsenų, konfliktams spręsti vis dažniau taikomos hibridinės priemonės, apimančios politinius, ekonominius, humanitarinius, informacinius ir kitus ne karinius metodus (Gerasimov, 2013). Šiuos teiginius Rusija praktiškai įgyvendino 2014 m. vykusios Krymo aneksijos metu, kai lygiagrečiai su skiriamųjų ženklų neturinčiomis specialiųjų pajėgų grupėmis, naudotomis užimti Ukrainos valstybines institucijas, organizavo kibernetines atakas prieš Ukrainos valstybinę logistinę ir informacinę infrastruktūrą, vykdė dezinformuojančius veiksmus socialiniuose tinkluose (Duggan, 2015). Esant tokiai situacijai bei atsiminus vienus ryškiausių pastarojo meto įvykius, kai kibernetinės priemonės buvo taikomos paveikti fizinėje erdvėje esančius procesus, pavyzdžiui, rinkimus JAV, sudėtinga būtų nesutikti su teiginiais, kad kibernetinis saugumas yra su valstybės suverenumu, nacionaliniu saugumu, kultūriniu paveldu bei gėrybėmis ir vertybėmis susijęs klausimas,

35 http://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1/

36 http://www.telegraph.co.uk/news/2017/06/27/cyber-attack-could-lead-military-retaliation-says-fallon/

atliekantis saugaus ekonominės plėtros garanto funkcijas (Ghernaouti, 2013). Atsižvelgiant į tai, kad nepaisant tęstinio rizikų valdymo progreso, kibernetinėje srityje visų potencialių atakų prognozavimas ir prevencija yra neįmanomas uždavinys dabartinėms ir netgi ateities kibernetinėms sistemoms (Linkov ir kt., 2013) bei tradicinių metodų, paremtų rizikų matricomis neveiksmingumą ir placebo įspūdžio sudarymą (Hubbard, Seiersen, 2016), būtina ieškoti būdų ir naujų požiūrių, kaip padaryti norimas apsaugoti sistemas atspariomis, galinčiomis absorbuoti kibernetines atakas, adaptuotis prie jų nuolatos keliamų iššūkių ir kuo greičiau po jų atsistatyti. Toks atsakas galėtų būti tarpdisciplininiu požiūriu paremti kibernetinio saugumo valdymo ir atsparumo tyrimai.

Mokslinė problema ir jos ištirtumo lygis. Nagrinėjant kibernetinio saugumo valdymo literatūrą, kurioje analizuojama kibernetinio atsparumo perspektyva, skirtinos kelios, šiam darbui aktualios teorinės iteracijos. Pirma – informacinių sistemų ir jose vykstančių procesų atsparumas, t.y. informacines sistemas veikloje naudojančių organizacijų atsparumas, dėl šių technologijų taikymo ir su jomis susijusių procesų vykdymo kylančioms grėsmėms. Antra – organizacijų, kaip visumos, atsparumas kibernetinėms grėsmėms. Vienas ankstyvesnių bandymų nagrinėti ir suprasti organizacijų atsparumą iš informacinių sistemų perspektyvos yra Riolli ir Savicki (2003) tyrimas, kurį patys autoriai pozicionuoja kaip atsaką į tuo metu šioje srityje buvusį teorinį vakuumą. Autorių darbas integruoja tuo metu egzistavusias individualaus, psichologinio ir organizacinio atsparumo teorijas. Nors šio tyrimo atveju įvardijamas sisteminis stresorius nėra kibernetinės organizacijai kylančios grėsmės, vertėtų akcentuoti tyrėjų išskirtus keletą svarbių faktorių, reikšmingų bendrojo kibernetinio atsparumo idėjų formavimui. Visų pirma, stresą organizacinei sistemai sukelia jos veiklos erdvėje egzistuojantys technologiniai pokyčiai, aukštas informacinių sistemų dinamikos laipsnis ir nuolatinė rinkų akceleracija. Antra, atsparumas būdamas sisteminiu faktoriumi, priklausomu nuo aibės organizacinės sistemos atributų, užtikrinamas tik individualiame lygmenyje negarantuoja visos organizacijos atsparumo. Būtina plėtoti abu lygius kaip visumą (Riolli, Savicki, 2003). Starr, Newfrock ir Delurey (2003), kalbėdami apie organizacijų atsparumą įtinklintos ekonomikos ir tinklinių organizacijų kontekste, akcentavo aibę atsparumo užtikrinimo faktorių, iš kurių skirtini: situacijos žinojimas, rizikų valdymas bei organizacijos struktūrinio sudėtingumo suvokimas. Starr, Newfrock ir Delurey (2003) pagrindiniu organizacinės sistemos stresoriumi įvardina bendrąsias rizikas, kylančias dėl tinklinėse struktūrose atsiradusių komunikacijos, tiekimo ir kitų sutrikimų. Milligan ir Hutcheson (2006) vertino informacinių technologijų teikimo taikant užsakomųjų paslaugų modelius (angl. *outsourcing*) įtaką organizacijos kibernetiniam atsparumui. Pažymėtina, kad Milligan ir Hutcheson (2006) tarp aibės kitų operacijų ir palaikymo rizikų išskiria ir loginio saugumo rizikas. Nors šios rizikos sudaro tik mažą bendrųjų organizacijos rizikų dalį, reikėtų akcentuoti, kad toks integruotas rizikų valdymas vertintinas, kaip pakankamai brandus rizikų valdymo požiūris. Kiek vėliau organizacijų atsparumą iš verslo valdymo sistemų perspektyvos nagrinėjo Ignatiadis ir Nandhakumar (2007). Vienas esminių tyrėjų teiginių yra toks: „Sudėtingos verslo valdymo sistemos dėl savo taikomų kontrolės mechanizmų yra rigidiškos prigimties, jos turi polinkį slopinti ir mažinti bendrąjį organizacijos lankstumą ir atsparumą“. Taip pat vertėtų išskirti Werfs ir Baxter (2013),

nagrinėjusių sociotechninės adaptyvias sistemas iš atsparumo perspektyvų, tačiau neakcentuojančių jų atsparumo būtent kibernetinėms grėsmėms.

Plėtojant diskusiją apie antrąją atsparumo tyrimų iteraciją, didžiausią aktyvumą įgavusią šio dešimtmečio pradžioje, reikia pažymėti, kad daugiausia dėmesio ją atstovaujantys tyrėjai skiria atsparumo metrikų formavimui bei atsparumo plėtojimui kritinės infrastruktūros sistemose; valdymo perspektyva kibernetinio atsparumo tyrimuose sutinkama ypač retai. Kalbant apie sisteminius kibernetinio atsparumo aspektus, vertėtų išskirti Goldman (2010), nagrinėjusios kritinių sistemų projektavimo, diegimo ir valdymo procesus iš atsparumo perspektyvos. Vienas esminių autorės teiginių yra raginimas suvokti, kad neįmanoma sustabdyti kibernetinių atakų, tačiau sistemų architektūros pertvarka taikant atsparumo požiūrius gali sumažinti atakos pasekmes, pakelti jų kainą puolančiajai pusei ir veikti kaip atgrasymo priemonė ateityje (Goldman, 2010). Kibernetinis atsparumas tyrinėtas ne tik kaip sisteminis elementas, bet ir kaip projektavimo objektas (Bodeau ir kt., 2012; Bodeau, Graubart, Laderman, 2014; Häring, Ebenhöch, Stolz, 2016; Sansavini, 2017). Literatūroje taip pat sutinkami bandymai tyrinėti kibernetinio atsparumo dinamiką skirtingose sisteminėse aplinkose: mažose verslo įmonėse (Williams ir Manheke, 2010), sveikatos apsaugos sektoriuje (Williams, 2010), debesų kompiuterijos sistemose (Thebeau ir kt., 2014), e. sveikatos sistemose (Liveri, Sarri ir Skouloudi, 2015), transporto srityje (Nogal ir O'Connor, 2017), elektros inžinerijoje (Zussblatt ir kt., 2017) tiekimo grandyse (Urciuoli, 2015), konkrečiuose geografiniuose ir politiniuose vienetuose (Kaufmann, 2015; Peter, 2017), politinio sudėtingumo perspektyvoje (Herrington ir Aldrich, 2013), organizacijos veiklos reputacijos išsaugojimo procesuose (Wilding, 2016). Taip pat vertėtų išskirti nemažą skaičių įvairių autorių suformuotų atsparumo matavimo modelių ir metrikų, skirtų išmatuoti organizacijos, sistemos, padalinio ar kito organizacinio vieneto atsparumą kibernetinėms grėsmėms (Wang ir kt., 2010; Allen, 2011; Ford ir kt., 2012; Linkov ir kt., 2013; Vugrin ir Turgeon, 2013; Houston ir Sicker, 2014; Bodeau ir Graubart, 2016; Friedberg ir kt., 2016; Shapiro, 2016; Häring ir kt., 2017; Heinimann ir Hatfield, 2017). Atskirai vertėtų pažymėti Tran ir kt. (2016) modelį, suformuotą įveikti nulinės dienos kenkėjiškos programinės įrangos keliamus iššūkius. Kalbant apie kibernetinio atsparumo tyrimus kritinės infrastruktūros sistemose, atsparumas šioje perspektyvoje nagrinėtas kaip nacionalinės ir korporatyvios socialinės atsakomybės elementas (Ridley, 2011), kompleksiškų kritinių infrastruktūrų sistemų pagrindas (Lewis, Mackin, Darken, 2011), kritinės infrastruktūros komponentas iš sociopolitinės ir procedūrinės perspektyvų (Lundborg ir Vaughan-Williams, 2011; Moteff, 2012), kaip pramonės procesų valdymo sistemų elementas (Krotofil ir Cárdenas, 2013; Chaves ir kt., 2017), kaip kritinės infrastruktūros absorbavimo, adaptavimosi ir veiklos atstatymo pagrindas (Setola, Luiijf, Theocharidou, 2016; Balutis ir kt., 2016), kritinės infrastruktūros socialinio atsparumo elementas (Trump ir kt., 2017), kritinės infrastruktūros viešojo ir privataus sektoriaus partnerystės objektas (Trucco ir Petrnej, 2017), konkrečios valstybės kritinės infrastruktūros apsektas (Todorovic ir kt., 2017).

Dėl egzistuojančio tyrimų fragmentiškumo ir suvokimo problematikos sudėtinga apibrėžti, kur baigiasi vienų organizacinių kibernetinio saugumo valdymo atsakomybių ribos ir prasideda kitų. Tai suformuoja būtinybę išgryninti esamą kibernetinio saugumo sąvokų terminiją ir nustatyti konceptualias kiekvieno šio reiškinio vartosenos ribas. Nagrinėjant

mokslinę literatūrą, teisės aktus, NATO ir ES bei aukščiausio lygmens politikų pasisakymus, galima teigti, kad bendroje kibernetinio saugumo valdymo technologinių komponentų aibėje kibernetinis atsparumas yra viena reikalingiausių šių laikų sociotechninių sistemų savybių, tačiau nėra pakankamai aišku, kokiomis priemonėmis ši savybė turėtų būti įgyvendinama, palaikoma ir didinama. Akivaizdu, kad kibernetinio atsparumo konceptualaus suvokimo ir įgyvendinimo principai skirtinguose sociotechniniuose junginiuose gali būti plėtojami skirtingai, įvertinant konkrečiame vienete egzistuojančią organizacinę kultūrą ir valdymo tradicijas. Visus šiuos teiginius galima apibendrinti **moksline problema**, išreiškiamą klausimu: „Kaip formuoti kibernetinio saugumo valdymo procesus, siekiant pagerinti organizacijų atsparumą kibernetinėms grėsmėms?“.

Tyrimo objektas – organizacijų kibernetinio saugumo valdymo gerinimas.

Tyrimo tikslas – suformuoti validuotą kibernetinio saugumo valdymo modelį paremtą atsparumo požiūriu.

Tyrimo uždaviniai:

1. Atlikus mokslinių šaltinių analizę atskleisti kibernetinių grėsmių dinamiką, kibernetinio saugumo ir atsparumo objektą, kibernetinio atsparumo valdymo aspektus, formavimo prielaidas ir kliūtis, identifikuoti esminius faktorius lemiančius kibernetinio saugumo aktualizavimą skirtinguose organizacijos valdymo lygmenyse.
2. Teorinių įžvalgų pagrindu suformuoti konceptualų kibernetinio saugumo valdymo modelį, integruojantį svarbiausius organizacijų kibernetinio atsparumo sisteminius ir valdymo faktorius.
3. Validuoti konceptualųjį kibernetinio saugumo valdymo modelį ir nustatyti svarbiausius jo konstrukcinius elementus, atliekant pusiau struktūrizuotą kibernetinio saugumo ekspertų interviu bei kokybinę Lietuvos kibernetinį saugumą reglamentuojančių teisės aktų analizę.
4. Modelio pagrindu pateikti praktines rekomendacijas, kaip galėtų būti gerinamas kibernetinio saugumo valdymas organizacijose, taikant kibernetinio atsparumo požiūrius.

Ginamieji teiginiai:

1. Kibernetinio saugumo tyrimų ir praktiniuose domenuose susiduriama su kibernetinio saugumo valdymo sampratos problematika, todėl būtinas šios srities terminijos išgryninimas, sąvokų suvienodinimas, kibernetinio saugumo praplėtimas sistemine ir valdymo perspektyvomis.
2. Kibernetio saugumo valdymo gerinimas neatskiriamas nuo bendro saugumo bendruomenės kibernetinio raštingumo lygio augimo, kibernetinio saugumo sistemos veikėjų gebėjimo keistis informacija procesų tobulinimo, tarpinstitucinio bendradarbiavimo skatinimo įvairiuose organizacinių sistemų valdymo lygmenyse.
3. Didėjant kibernetinių atakų skaičiui ir augant jų sudėtingumo lygiui, viena aktualiausių sistemos savybių tampa atsparumas, todėl skatintinas atsparumo požiūriu paremtas kibernetino saugumo valdymas. Kibernetinio saugumo valdymas tobulintinas taikant parengtą kibernetinio saugumo valdymo gerinimo modelį.

4. Kibernetinio atsparumo plėtra organizacijose sąlygoja bendrąją organizacijos, kaip sociotechninės sistemos, evoliuciją, didina sistemos teikiamų paslaugų gavėjų pasitikėjimą sistema.

Disertacinio darbo tyrimo metodai:

Teoriniai metodai. Siekiant suformuoti kibernetinio saugumo valdymo modelio teorinį pagrindą buvo vykdoma mokslinės literatūros analizė, kurios metu taikyti sisteminimo, sintezės, lyginimo bei apibendrinimo metodai. Modelio suformavimui taikyti konceptualiojo modeliavimo ir vizualizacijos metodai.

Empiriniai metodai. Modelio validacijai taikyti vienas kitą papildantys kokybiniai empiriniai tyrimai: ekspertinis interviu, kokybinė turinio analizė, antrinių šaltinių duomenų analizė.

Mokslinė darbo vertė ir mokslinis darbo naujumas. Darbe taikant tarpdisciplininį, holistinį požiūrį praplėstas egzistuojantis kibernetinio saugumo valdymo ir atsparumo tyrimų diskursas, įtraukiant į jį organizacinius ir valdymo aspektus. Darbe išgrynintos kibernetinio atsparumo suvokties ribos, išskirti pagrindiniai organizacijų kibernetinio atsparumo elementai. Organizacijų atsparumas kibernetinėms grėsmėms išnagrinėtas keliais valdymo lygmenimis, taip sudarant prielaidas tolimesnei kibernetinio atsparumo procesų ir jų metu vykdomų sąveikų analizės plėtotei. Darbu daromas mokslinis indėlis į bendrą kibernetinio saugumo valdymo tyrimų lauką, formuojamos prielaidos tolimesniam reiškinio tyrinėjimui.

Praktinė darbo reikšmė. Darbas atskleidžia egzistuojančias kibernetinio saugumo valdymo problemas ir pasiūlo priemones joms spręsti, taikant atsparumu paremtus požiūrius ir tokiu būdu pagerinant kibernetinio saugumo valdymą viešojo sektoriaus organizacijose Lietuvoje. Nuolatos vis dažnėja raginimai didinti sistemų atsparumą kibernetinėms grėsmėms, tačiau praktiškai nėra metodikų, aprašančių, kaip šie procesai turėtų būti įgyvendinami. Suformuotas organizacijų kibernetinio saugumo modelis taikytinas plėtojant kibernetinio atsparumo iniciatyvas organizacijose įvairiuose valdymo lygmenyse.

Reikšminiai žodžiai: informacinis saugumas, kibernetinis saugumas, kibernetinio saugumo valdymas, kibernetinis atsparumas, kibernetinės grėsmės, atsparumo modelių taikymas kibernetinio saugumo valdymui gerinti.

Disertacinio darbo struktūra. Disertacinio darbo struktūra, kuri yra grindžiama tyrimo tikslu ir uždaviniais, pateikiama 1 paveiksle.

Šaltinis: *parengta autoriaus*

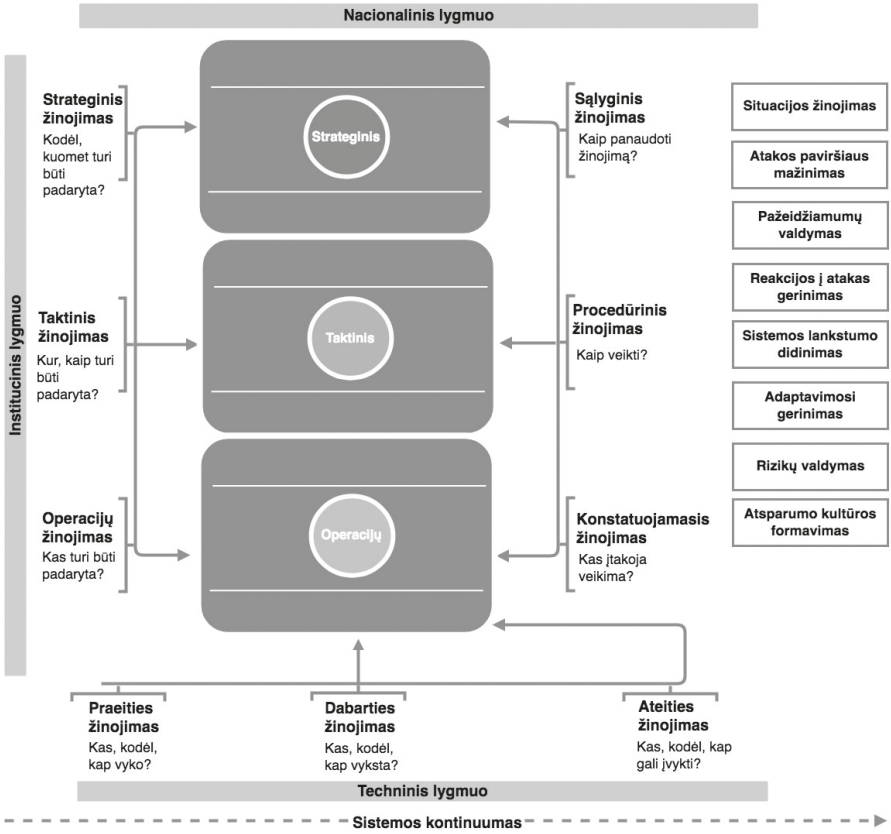
1 pav. *Disertacijos loginė struktūra*

Pirmojoje teorinėje disertacijos dalyje nagrinėjama saugumo reiškinio transformacija, atskleidžiama, kas sąlygojo poreikį konceptualiai permąstyti informacinio saugumo reiškinį bei ieškoti naujų, valdymo elementus integruojančių kibernetinio saugumo veiklų organizavimo būdų. Apžvelgiama kibernetinėje erdvėje kylančių grėsmių dinamika, įvertinama kibernetinio saugumo valdymo metodų kaita bei naujų, atsparumu pagrįsto valdymo požiūrių taikymo poreikis. Antrojoje disertacijos dalyje aprašoma atlikto empirinio tyrimo ir pasirinktų Lietuvos Respublikos kibernetinį saugumą reglamentuojančių

teisės aktų tyrimo metodika. Trečiojoje darbo dalyje pateikiami atlikto empirinio tyrimo rezultatai ir validuotas kibernetinio saugumo valdymo taikant atsparumo požiūrius konceptualus modelis, integruojantis esminius organizacijos kibernetinio atsparumo užtikrinimo elementus.

Patikslintas kibernetinio atsparumo modelis

Atlikus ekspertų interviu, visi išskirti modelio konstrukciniai elementai patvirtinti. Kaip parodė Lietuvos Respublikos pagrindinių kibernetinį saugumą reglamentuojančių teisės aktų analizė, juose reglamentuota tik dalis atsparumo principų. Todėl, būtina siūlyti naujus mechanizmus, kurie galėtų papildyti esamų priemonių visumą, vienas jų – patikslintas ir papildytas organizacijų kibernetinio atsparumo kibernetinėms grėsmėms modelis, pateikiamas 28 paveiksle.



Šaltinis: *parengta autoriaus*
2 pav. *Patikslintas kibernetinio atsparumo modelis*

Tyrime dalyvavę ekspertai pabrėžė būtinybę vykdyti komunikaciją visomis organizacijos hierarchijos vertikalės kryptimis, todėl kibernetinio atsparumo modelyje skirtini trys

organizacinės sistemos kibernetinio saugumo žinojimo ir bendradarbiavimo lygmenys: strateginis, taktinis ir operacijų. Nei viena valstybinė organizacija nevykdo savo veiklos vakuume, ji yra veikiama bendroje institucinėje sistemoje ir nacionaliniame kontekste vykstančių procesų. Organizacijos savo veiklas vykdo naudodamos IRT, dėl netinkamas jų organizavimo bei apsaugos kyla rizika, kad organizacijų veikla gali būti sutrikdyta. Šiems faktoriams apibrėžti modelyje išskiriami papildomi trys lygmenys: institucinis, nacionalinis ir technologijų. Ekspertų teigimu, kritiškai svarbūs elementai, siekiant padidinant organizacijos atsparumą, yra žinojimas ir komunikacija. Siekiant kuo geriau apimti žinojimo dimensijas, modelyje išskiriami devyni vienas kitą proceso dalyvių komunikacijos ir bendradarbiavimo metu papildantys žinojimo lygmenys:

- Organizacijos hierarchinio žinojimo lygmuo:
  - Strateginis žinojimo lygmuo – šiame lygmenyje formuojamas žinojimas, dėl ko vykdomos vienos ar kitos kibernetinio saugumo veiklos, nustatomos gairės jų įgyvendinimui.
  - Taktinis žinojimo lygmuo – formuojamas žinojimas apie priemones, kuriomis turėtų būti vykdomas strateginiame lygmenyje suformuotų užduočių įgyvendinimas.
  - Operacijų žinojimo lygmuo – konkrečių veiksmų įgyvendinimo žinojimas.
- Analitinis žinojimo lygmuo:
  - Praeities žinojimas – praėjusių kibernetinių grėsmių, incidentų, jų šalinimo būdų žinojimas, skaitmeninės ekspertizės (angl. *digital forensics*) veikla, po incidentinė peržiūra (angl. *post incident review*), išmoktų pamokų įvertinimas.
  - Dabarties žinojimas – stebėsena, įsibrovimo detektavimo sistemų informacijos valdymas, sistemos anomalijų analizė.
  - Ateities žinojimas – prognozavimas, nuspėjamoji duomenų analizė, ateities įžvalgos (angl. *foresight*).
- Meta-kognityvinis žinojimas (Schraw, 1998):
  - Sąlyginis žinojimas – žinojimas, kaip panaudoti turimas kibernetinio saugumo žinias.
  - Procedūrinis žinojimas – žinojimas, kaip vykdyti atliekamas užduotis iš kibernetinio saugumo perspektyvų.
  - Konstatuojamasis žinojimas – žinojimas, kaip padidinti turimas žinias, kokie faktoriai gali įtakoti žinių formavimą.

Taikant šį modelį, reikėtų įvertinti kiekvieną jo struktūrinį komponentą (situacijos žinojimas, atakos paviršiaus mažinimas ir kt.) visų žinojimo bei veiklos lygmenų kontekste.

IŠVADOS IR REKOMENDACIJOS

1-asis uždavinys.

1. Didėjant informacinių ir ryšio technologijų skverbčiai įvairiose žmonių veiklos srityse, intensyvėjant kibernetinėms atakoms didėja organizacijų patiriamos

žalos mastas. Grėsmių poveikis stiprėja ne tik virtualiose, bet ir fizinėse aplinkose esančioms vertybėms ir infrastruktūroms; vis dažniau sutrikdoma valstybinių institucijų, ligoninių, finansų sektoriaus bei kritinių paslaugų teikimą vykdančių infrastruktūrų veikla. Tai sąlygoja būtinybę vertinti kibernetines grėsmes iš sisteminės perspektyvos, svarbus ne tik saugumo objekto suvokimo poslinkis nuo siauro technologinio požiūrio link įvairias valdymo sritis apimančios traktuotės, bet ir aktualizavimas bendrame nacionalinio saugumo lygmenyje.

2. Kibernetinio saugumo diskurse egzistuoja tam tikras terminijos sąmyšis – nėra pakankamai aiškių nusistovėjusių sąvokų. Su ankstyvajam saugumo laikotarpiui būdingais, tačiau vis dar vartojamais terminais, tokiais kaip informacinis saugumas, el. informacijos sauga, naudojamos ir vėlesniems saugumo laikotarpiams būdingos sąvokos: kibernetinis saugumas, kibernetinis incidentas. Todėl prieš egzistuojančią terminiją papildant naujais konceptais, būtina apibrėžti ir suvienodinti esamą sąvokų terminų sistemą, suformuoti jų konceptualias sąsajas.
3. Kibernetinio saugumo ir atsparumo reiškinių suvokimo plėtotė vyksta augant tam tikros saugumo bendruomenės kibernetinio saugumo raštingumo lygiui. Ypač svarbu, kad vartosenoje esantys kibernetinio saugumo apibrėžimai tam tikros kibernetinio saugumo bendruomenės atstovų būtų suprantami vienodai. Prieš vykdant bet kokį sąvokų kategorizavimą, būtina įvertinti, ar tai neturės neigiamo poveikio šių sąvokų apimamiems kibernetinio saugumo objektams, neįvyks konceptualus jų atskyrimas iš bendrojo saugos konteksto, nes tai galėtų sąlygoti neigiamas pasekmes šių objektų finansavimui, plėtrai, bendram jų svarbos vertinimui.
4. Kibernetinio atsparumo valdymo esmę sudaro aibė sisteminių veiksnių, tačiau esminiais komponentais laikytini adaptavimosi, absorbavimo ir atsistatymo gebėjimai, kurių ugdymas leidžia išvengti sistemos funkcionavimo poslinkio nuo judėjimo link nepageidaujamos sisteminės konfigūracijos, kai ji yra veikiama išorinio arba vidinio stresinio faktoriaus, planuoto ar neplanuoto pokyčio.
5. Vienas pagrindinių iššūkių formuojant kibernetinio saugumo sistemų atsparumą yra būtinybė užtikrinti šių sistemų apsaugai taikytų priemonių, jų efektyvumo ir kitų valdymo bei sisteminių parametrų slaptumą, tai sąlygoja informacijos silosą, gerosios praktikos dalinimosi trikdžius. Todėl, ypač svarbu užtikrinti tinkamą apsikeitimą informacija tarp organizacijos valdančiosios grandies ir kibernetinį saugumą užtikrinančių padalinių.
6. Nors kibernetinis atsparumas dažnai nagrinėjamas sudėtingų adaptyvių sistemų perspektyvoje, jam formuoti dažnai būtinas sisteminis, tarpsektorinis požiūris, tačiau jo plėtojimas turėtų būti vykdomas laikantis proporcingumo, priemonių adekvatumo ir sisteminio paprastumo principų.
7. Resursų paskirstymas ir veiklos prioritetų nustatymas turi tiesioginę įtaką kibernetiniam atsparumui, todėl kibernetinis atsparumas ir saugumas turėtų būti vertinami ir plėtojami lygiagrečiai su kitais organizacijos veiklos procesais. Nustatant finansavimo prioritetus, jiems turėtų būti suteikiamas toks pats svarbos lygmuo.
8. Atsparumo kaitos dinamika teigiamai įtakoja bendruosius organizacijos procesus, prisideda prie organizacijos evoliucionavimo. Kibernetinio atsparumo plėtrai

organizacinių sistemų viduje svarbi tinkama ir savalaikė komunikacija, tarpinstitucinis bendradarbiavimas, aiškus veiklų pasidalijimas, dubliavimo vengimas. Taip pat labai svarbi kibernetinio atsparumo suvokimo sklaida, kuri turėtų būti vykdoma institucijų hierarchijos vertikale iš viršaus žemyn. Tinkamo lygio kibernetinio saugumo priemonių įgyvendinimas valstybinėse informacinėse sistemose didina piliečių pasitikėjimą valdžia, todėl aktuali ir išorinė komunikacija – kibernetinio atsparumo plėtrai nacionaliniu mastu būtinas valdžios bendradarbiavimas su visuomene.

9. Siekiant konkretizuoti kibernetinio saugumo ir atsparumo reiškinius bei nustatyti jų konceptualias ribas, būtina plėtoti šios srities diskusiją tarp įvairias kompetencijų sritis atstovaujančių kibernetinio saugumo ekspertų. Siekiant nustatyti tolimesnes organizacijų kibernetinio atsparumo formavimo tendencijas, kibernetinių grėsmių transformacijos tendencijas bei identifikuoti naujus atsparumo taikymo modelius, rekomenduojama vykdyti nuolatinius, tarpdalykinius kibernetinio atsparumo srities tyrimus. Ypač rekomenduotinos absorbavimo reiškinio įvertinimo studijos.

2-asis uždavinys.

1. Organizacinio ir sistemų atsparumo sričių konceptai yra mobilūs, todėl didžioji dalis šių sričių atsparumo formavimo principų taikytini formuojant kitų domenų atsparumo modelius.
2. Nepaisant to, kad pastaruoju metu ryšio ir komunikacijų technologijos yra pakankamai išplėtotos, egzistuoja informacinių silososų, kuriuose izoliuojami ne tik bendriniai informaciniai srautai, bet ir su kibernetiniu saugumu susijusi informacija, išlikimo tendencija. Todėl, vienas svarbiausių uždavinių organizacijų kibernetiniam atsparumui didinti – kibernetinio saugumo situacijos žinojimo gerinimas.
3. Organizacijos išgyvenimui grėsmę keliančių kritinių pažeidžiamumų identifikavimas, proaktyvus jų valdymą ir su jais susijęs reagavimas yra lemiami veiksniai siekiant užtikrinti tinkamą veiklos tęstinumo ir krizių valdymo srityje.
4. Vienas pagrindinių atsparumo principų yra adaptyvumas, kurio ugdymas gerina organizacijos gebėjimus judėti nuo reaktyvaus atsako link proaktyvaus pasirengimo ir gebėjimo veikti didelio nežinomumo sąlygomis.
5. Sistemos lankstumas – vienas esminių, sistemos atsparumą užtikrinančių faktorių, papildančių jos gebėjimą adaptuotis prie kibernetinių grėsmių, pertvarkant procesus bei sistemas pagal egzistuojančius kibernetinio saugumo situacijos poreikius.
6. Atsižvelgiant į kibernetinių atakų įvairialypę prigimtį, organizacijos atakos paviršiaus mažinimas turi būti vykdomas kompleksiškai, integruojant sisteminius ir žmogiškuosius faktorius.
7. Vykstant vis glaudesnei socio-fizinių ir techninių sistemų konvergencijai, reakcijų į atakas procesų gerinimas yra ypač aktualus sisteminio atsparumo komponentas.
8. Kylantis kibernetinių sistemų ir joms kylančių grėsmių sudėtingumo lygis reikalauja organizacinių bei techninių rizikų ir atsparumo valdymo procesų integracijos.

3-iasis uždavinys.:

1. Pradiniai pateikto kibernetinio atsparumo modelio komponentai: kibernetinio saugumo situacijos žinojimo gerinimas, esminių pažeidžiamumų valdymo gerinimas, adaptyvių gebėjimų gerinimas, sistemos lankstumo gerinimas, reakcijos į atakas gerinimas, atakos paviršiaus mažinimas, rizikų valdymo gerinimas, yra validūs ir taikytini formuojant konceptualųjį organizacinio atsparumo kibernetinėms grėsmėms modelį.
2. Vertinant iš žmogiškųjų kibernetinio saugumo situacijos žinojimo perspektyvų, situacijos žinojimo gerinimas turėtų būti įgyvendinamas vykdant visų grandžių darbuotojų mokymus, paremtus praktiniais kibernetinio saugumo pavyzdžiais ir aktyviu jų dalyvavimu realiomis situacijomis bei suformuotais situacijos paaiškinimais paremtose pratybose.
3. Siekiant įgyvendinti tinkamus pasirengimo atakoms mechanizmus, būtina žinoti ne tik dabartinę kibernetinio saugumo situaciją, bet ir gebėti numatyti galimas kibernetinio saugumo grėsmes ateityje, rekomenduojama suformuoti kibernetinių grėsmių analizės mechanizmus valstybės mastu, padėsiančius prognozuoti potencialias grėsmes ir atsižvelgiant į gautą informaciją proaktyviai formuoti kibernetinės gynybos elementus.
4. Ypač svarbus veiksnys bendram kibernetinio saugumo situacijos žinojimui yra geopolitinės informacijos vertinimo mechanizmų diegimas, skirtų stebėti geopolitinę situaciją iš kibernetinio saugumo perspektyvos. Taip pat būtina vykdyti sisteminę kibernetinių nusikaltėlių, jų organizacijų stebėseną. Rekomenduojama suformuoti šias funkcijas vykdantį organizacinį vienetą, kuris pagal kompetenciją dalintųsi informacija su suinteresuotomis šalimis.
5. Siekiant didžiausio esminių pažeidžiamumų valdymo efekto organizacijoje, esminių pažeidžiamumų suvokimas turi būti formuojamas aukščiausiu tam tikros organizacijos valdymo lygmeniu, aiškiai pozicionuojant pažeidžiamumo objektus visoje būtinų apsaugoti elementų sistemoje.
6. Visų esminių pažeidžiamumų valdymo gerinimo priemonių aibėje būtina akcentuoti personalo mokymus, kurių pagalba būtų ugdoma bendra organizacijos, sektoriaus ar valstybės kibernetinio saugumo kultūra bei mokoma tinkamos kibernetinės higienos palaikymo ne tik sisteminiame, bet ir eilinio vartotojo lygmenyje.
7. Viena priemonių pažeidžiamumų valdymui gerinti – tai vertybių inventorizacijos ir sąrašų sudarymo vykdymas organizacijoje, jų tarpusavio sąsajų suvokimas. Esminių pažeidžiamumų valdymo poreikiai geriausiai perteikiami per jų sąsajas su organizacijos vykdoma veikla bei finansine dedamąja – tuomet atsiranda svarus, gerai visoms organizacijos grandims suvokiamas pagrindimas egzistuojantiems poreikiams.
8. Pakankamo esminių pažeidžiamumų valdymo svarbos nesuvokimas kelia dvejopas problemas:
    - egzistuoja tikimybė nesulaukti pritarimo, kad būtina šalinti pažeidžiamumus;
    - egzistuoja atvirkštinės manipuliacijos tikimybė, t.y. investicijų skyrimas ten, kur jų visai nereikėtų.

9. Esminių pažeidžiamumų valdymui būtina pasiekti konsensą ir bendrą situacijos suvokimą tarp IT padalinių, atliekančių sistemos tvarkymą ir sistemos valdytojo, pavyzdžiui, ministerijos; būtinas vienodas suvokimas, kad, visų pirma, turėtų būti vykdomas silpnų vietų šalinimas, o tik vėliau – plėtra. Saugos priemonių plėtojimą visų tipų organizacijose rekomenduojama vykdyti bent jau lygiagrečiai su plėtra, o ne po jos.
10. Adaptacijos gerinimo procesai turėtų prasidėti prieš įvykstant krizinėms situacijoms ar organizacijos teikiamų paslaugų lygio nuosmukiams. Dalis adaptacijos mechanizmų rekomenduojama atspindėti veiklos tęstinumo planuose, numatant scenarijus, apibrėžiančius visas galimas veiklos kryptis krizinių situacijų atvejais; rekomenduojama vykdyti esamų veiklos tęstinumo priemonių tobulinimą.
11. Vienas efektyviausių adaptavimosi gerinimo priemonių – pratybos, iš jų ir veiklos atkūrimo bei atsistatymo iš atsarginių kopijų pratybos. Siekiant padidinti pratybų vykdymo efektyvumą, būtina tobulinti pratybų atlikimo mechanizmus ir taip sumažinti vidinį pasipriešinimą dėl darbuotojų laiko gaišinimo ir dėl pratybų atsiradusių papildomų užduočių. Vertinant bendrąsias adaptavimosi tendencijas Lietuvoje, reikėtų konstatuoti, kad organizacijoms labiau būdinga reaguoti nei adaptuotis ar pasirengti. Ši sritis tobulintina kartu su po incidentinių įvykių peržiūra.
12. Sistemos lankstumui užtikrinti ypač svarbus elementas yra žmogiškasis faktorius, taigi kiek žmogus išliks rigidiškas savo požiūriais, ketinimais ir t.t., tiek nelanksti bus ir sistema. Sistemos lankstumui taip pat ypač svarbi organizacijos vadovybės kompetencija, nes, priešingu atveju, nekompetentingas vadovas gali duoti nurodymus sistemose naudoti esamus komponentus, kurie galbūt visiškai netinkami jos lankstumui ir atsparumui gerinti.
13. Bandymas pasiekti lankstumą atnaujinamose, iš prigimties statiškose sistemose gali duoti neigiamų rezultatų, todėl norint sistemas suformuoti lanksčiomis, rekomenduojama jas kurti iš pagrindų, nes, priešingu atveju, rigidiškai sistemai pereiti iš statiškos į lanksčią bei suformuotą moduliais gali būti pernelyg sudėtinga.
14. Prieš priimant sprendimus dėl specifinių saugumo priemonių taikymo būtina įvertinti, ar ši priemonė pakankamai efektyvi atsakyti į egzistuojančius saugumo iššūkius, kai kibernetinė priešprieša tarp atakuojančiųjų ir besiginančiųjų šalių evoliucionuoja nuo paprasto kibernetinio incidento link sisteminių kibernetinių karinių veiksmų, todėl atsiranda poreikis konceptualiai pakelti reagavimo veiksmus į kibernetinės gynybos (angl. *cyber defence*) lygmenį.
15. Kritiškai svarbu reakcijai į atakas – saugumo politikos apibrėžimas organizacijoje; apibrėžtos reaguojant į atakas naudojamos įrangos taikymo procedūros.
16. Dažnai pernelyg didelis dėmesys skiriamas organizacijos atakos paviršiaus mažinimui iš išorinių grėsmių perspektyvos, tačiau dažnai neįvertinamas labai svarbus ir gana pažeidžiamas bei silpnas organizacinės sistemos elementas – žmogiškasis faktorius.
17. Augant socialinės inžinerijos atakoms ypač aktualūs yra darbuotojų mokymai ir jų švietimas, kuris, kartu su kibernetinės higienos ugdymu ir procedūriniais mechanizmais, yra viena iš pagrindinių priemonių atsižvelgiant į emocijomis

besivadovaujančių žmonių prigimtį. Mokymus rekomenduojama vykdyti sudarant galimybę personalui realiai sudalyvauti simuliuojamuose atakose, vėliau parodant rezultatus ir atrastas saugumo spragas; tokios priemonės turi potencialą tapti veiksmingesnėmis suvokimo apie kibernetinio saugumo būklę formavimui nei formalių mokymo metodų naudojimas.

18. Organizacijoje rizikų visumos valdymas yra vienas iš pagrindinių uždavinių, nepaisant kokio pobūdžio rizikos tai bebūtų. IT rizikos yra bendra visų rizikų dalis, tad jos valdymas turi būti integruotas į visų kitų organizacijai kylančių rizikų visumą; tik aukštą rizikų valdymo kultūrą turinti organizacija geba integruotai valdyti visas rizikas, jų nediversifikuodama. Atsižvelgiant į tendenciją, kad atsiranda atvejų, kai su į IT sritimi susijusias problemas kitos organizacijos dalys įsiklausyti nenori, rekomenduojama tai gerinti formuojant organizacijos kibernetinio saugumo kultūrą, požiūrį į kibernetinio saugumo keliamas problemas, didinant bendros kibernetinio saugumo problematikos suvokimą. Atsiradus suvokimui organizacijoje stiprėja rizikų valdymo ir kibernetinio saugumo gerinimo inercija. Rizikų valdymas turėtų egzistuoti sistemos palaikymo ir jos gyvavimo procesuose iki neigiamų veiksnių sukeliamo sistemos veiklą trikdančio poveikio ir būtent tinkamai atliktas rizikų valdymas padėtų sugrįžti jai į pradinę būseną.
19. Rizikų valdymas yra tiesiogiai susijęs su kompanijos, organizacijos, aljanso narių skirtingų padalinių gebėjimo bendradarbiauti ir keistis informacija. Tai apima informacijos sklaidą ir viešinimą apie procesus, vykdomas darbines veiklas, naudojamą įrangą ir kt. Jeigu šie procesai nevykdomi, organizacijos nariai nesupranta pavojų, jei šie pavojai tinkamai neįvertinami, yra sudėtinga apibrėžti rizikas, kurios galėtų atsirasti organizacijos sistemose, skirtingiems padaliniams vykdant tik jiems žinomas veiklas. Kuo daugiau personalas žinos kas vyksta, kokios sistemos dalyvauja ir kaip jos tarpusavyje susijusios, tuo bus geresnis rizikos valdymas. Taigi, rizikų valdymo vienas iš esminių uždavinių – įtraukti kuo daugiau žmonių į rizikos valdymo procesą iš skirtingų organizacijos veiklos sektorių, neapsiribojant vien IT. Viešajame sektoriuje Lietuvoje egzistuoja tendencija visus su kibernetinio saugumo sritimi susijusius rizikų valdymo veiksmus deleguoti IT padaliniams. Tačiau saugos ir IT padaliniai gali suteikti reikiamas pagalbines priemones, o IT rizikų vertinimą turi atlikti organizacijos veiklos procesus vykdanti jos dalis.
20. Pats rizikų valdymo procesas Lietuvos viešajame sektoriuje neblogai reglamentuotas, tačiau rekomenduojama atnaujinti metodines priemones; kasmet atliekami rizikų vertinimai ganėtinai formalūs; į bendrą rizikų procesą rekomenduojama įtraukti daugiau organizacijos atstovų, ne tik saugos įgaliotinius.
21. Vertinant iš atsparumo perspektyvos, Lietuvos Respublikos teisės aktuose, reglamentuojančiuose kibernetinį saugumą išsamiausiai apibrėžti atsparumo domeno planavimo ir pasirengimo principai; stokojama Absorbavimo, Detektavimo ir Atsistatymo dimensijas apimančių atsparumo nuostatų formalizavimo. Formuojant naujus kibernetinį saugumą reglamentuojančius teisės aktus, rekomenduojama didesnį dėmesį skirti kognityviniams atsparumo aspektams bei visų atsparumo dimensijų Absorbavimo, Detektavimo ir Atsistatymo fazėms.

Publikacijos:

Grincevicius R. (2013). Mobile Government: Application, Development Factors and Future Perspectives. Social Technologies, 13, ISBN 978-9955-19-586-3.

Grincevicius R. (2012). Foresight As A Part of e-Government Strategic Planning Process: The Foresight Model. Social Technologies, ISSN 2029-7564, 2(1), p. 114–128.

Konferencijos:

Role of The Foresight in The e-Government Strategic Planning, Social technologies 2010.

Mobile Government: Application, Development Factors and Future Perspectives.

Projektai:

Tarptautiškumas viešojo administravimo studijose

Vardas, pavardė	Rokas Grincevičius
El. pastas:	rokas.grincevicius@gmail.com

Išsilavinimas:

2008-2010	E.valdžios administravimo magistras Mykolo Romerio universitetas

Moksliniai interesai: informacinis saugumas, kibernetinis saugumas, atsparumas, e.valdžia

Darbo patirtis:

2018-07 – dabar	Vyresnysis techninis konsultantas, Europos išorės veiksmų tarnyba/Fujitsu Belgija
2017-08 – 2018-06	Sprendimų architektas, UAB „COWI Lietuva“
2016-03 – 2017-07	Platformos inžinierius, „Danske Bank“ filialas Lietuvoje
2013-07 – 2016-03	Operacijų integravimo vadovas, „Barclays Group Operations Limited“
2013-05 – 2013-12	Vyriausiasis specialistas, Lietuvos Respublikos vidaus reikalų ministerija
2010-12 – 2012-06	Lektorius, Mykolo Romerio universitetas
2007-09 – 2009-12	Duomenų bazių produktų vadovas, UAB „Lintel“
2005-10 – 2007-09	Projektų vadovas, UAB „Senukų prekybos centras“

MYKOLAS ROMERIS UNIVERSITY

Rokas Grincevičius

IMPROVEMENT OF CYBER SECURITY MANAGEMENT USING RESILIENCE MODELS IN ORGANISATIONS

Summary of Doctoral Dissertation
Social Sciences, Management (03 S)

Vilnius, 2019

The doctoral dissertation was prepared at Mykolas Romeris University during 2012–2018 under the right to organize doctoral studies granted to Vytautas Magnus University together with Klaipėda University, Aleksandras Stulginskis University, Mykolas Romeris University and Šiauliai University by the order of the Minister of Education and Science of the Republic of Lithuania No. V-1019 dated on June 8, 2011.

Scientific supervisor: Prof. Dr. Aelita Skaržauskienė (Mykolas Romeris University, Social Sciences, Management, 03S).

The doctoral dissertation will be defended at the Scientific Council of Vytautas Magnus University, Klaipėda University, Mykolas Romeris University and Šiauliai University in the field of Management:

Chairman:
Prof. Dr. Tadas Limba (Mykolas Romeris University, Social Sciences, Management, 03S)

Members:
Prof. Dr. Audrius Gargasas (Vytautas Magnus University, Social Sciences, Management, 03S);
Prof. Dr. Sandro Gerić (Zagreb University, Croatia, Technology Sciences, Informatics Engineering, 07T);
Prof. Dr. Diana Šaparnienė (Šiauliai University, Social Sciences, Management, 03S);
Prof. Dr. Darius Štitilis (Mykolas Romeris University, Social Sciences, Law, 01S).

The doctoral dissertation will be defended at the open meeting of the Scientific Council in the field of Management on April 12th, 2019 at 10:00 at Mykolas Romeris University, I-414 Room.
Address: Ateities g. 20, 08303, Vilnius, Lithuania.

The summary of the doctoral dissertation was sent on March 12th, 2019.

The Doctoral Dissertation is available at Martynas Mažvydas National Library of Lithuania (Gedimino st. 51, Vilnius), Klaipėda University library (K.Donelaičio a. 3, Klaipėda), Mykolas Romeris University library (Ateities st. 20, Vilnius), Šiauliai University library (Vytauto st. 84, Šiauliai), Vytautas Magnus University library (K.Donelaičio st. 52, Kaunas).

INTRODUCTION

Relevance of the topic. Transformation of various human activities from the physical to the cyber space caused not only the convergence of physical and cyber domains, but also disappearance of boundaries between traditional and cyber crimes. With the rise of new digital business models, criminals also discovered new forms of crime in which electronic assets and data can be both a target or a tool of criminal activity. Offenses, cases of industrial and political espionage, cyber terrorism attack against individuals, organisations, states, critical infrastructure are on the raise and are increasing every year. In June of 2017 a massive cyber attack was launched against businesses, airports, banks and public institutions in Ukraine, which later spread to other European countries, including Lithuania. This was the second cyber attack, which was launched only few weeks after the *WannaCry* ransom ware attack, and affected not only single organisations, but also the critical systems such as the United Kingdom's National Health Service. Sir Michael Fallon, the United Kingdom's Secretary of Defence warned the attackers that the United Kingdom could respond with the conventional military strikes to the future cyber attacks. "Cyber attacks could cause the response from any of the domains: air, land, sea or cyberspace", stated the Secretary. Such issues are causing not only the disruption of various businesses, but also huge financial losses. According to forecast made by the UK's Lloyd's of London insurance market, global cyber-attacks cost 400 billion yearly (Hubbard, Seiersen, 2016). The global insurance company XL Catlin, which in their product line has the insurance from cyber threat caused loses, described the cyber threats as the biggest systemic threats the company has seen over its 40-year-old practice in insurance business (Z/Yen Group, 2015). Cybercrime also increasingly becomes a tool for geopolitical conflict, widely used in the context of newly emerging unconventional forms of warfare. As Russian General Staff Valery Gerasimov noted that the XXI century wars are no longer declared, and hybrid instruments involving political, economic, humanitarian, information and non-military approaches are increasingly being used in the conflicts which have no clear margins between states of war and peace (Gerasimov, 2013). These statements were implemented by Russia in practice in 2014 during the Crimean annexation, when their state controlled hackers organised cyber attacks against the Ukrainian state logistical and information infrastructure along with the Russian special forces which were used to occupy the Ukrainian state authorities. All this happened in parallel with the disinformation and fake news in social networks (Duggan, 2015). In the context of one of the most striking recent events, when cyber space means were used to influence the processes of physical space during US elections, it would be difficult to disagree with the statements that cyber security is closely related to state's sovereignty, national security, cultural heritage, and assets and also serves as a guarantee of secure economic development (Ghernaouti, 2013). Taking into account the fact that despite the continuous progress in the area of cyber risk management, it is impossible for current and even for the future cyber security systems to predict and to prevent all potential cyber attacks (Linkov et al. 2013). Some researches acknowledge that traditional risk matrix based cyber security management methods, are ineffective and only create placebo effect (Hubbard, Seiersen, 2016), this determines a necessity to find the new security

approaches, which could help to protect the systems, to make them resilient, capable to absorb the cyber attacks, to adapt to the challenges caused by the attacks and to restore their activity as soon as possible after the attacks. Such new approach could be the interdisciplinary resilience based research.

Scientific problem and the level of its research. Analysis of cyber security literature, related to cyber resilience, shows that several theoretical cyber resilience iterations exist. The first one covers resilience of information systems and their processes, i.e. the resilience of the organisations, which are using the information systems, to cyber threats caused by the usage of these technologies and the processes related to application of the technologies. The second iteration covers the resilience of organisations to the cyber threats. One of the earliest attempts to explore and understand the resilience of organisations from the perspective of information systems is Riolli and Savicki's (2003) work, which is positioned by the authors as an attempt to respond to the existing theoretical vacuum of that time. The work of the authors integrated the theories of psychological, individual and organisational resilience. Despite the fact that in the Riolli and Savicki's (2003) case the main systemic stressor to the organisation is not the cyber threats, it is worth noting that the authors identified a set of important factors, which are critical to the formation of general cyber resilience. According to the authors stress to organisation is caused by technological changes in its operational space, a high degree of dynamism of information systems and the continuous acceleration of markets. Resilience is a systemic factor, which depends on the attributes of the organisational structure, so development of the resilience at the individual level does not guarantee the resilience of organisation as a whole. It is necessary to develop both levels (Riolli, Savicki, 2003). Analysing the resilience of organisations in the context of integrated economies and network organisations, Starr, Newfrock, and Deloirey (2003) emphasised a set of resilience factors that include: situational awareness, risk management and perception of the organisation's structural complexity. The main stressor to organisational systems, identified by Starr, Newfrock, Delurey (2003) is the whole of general risks caused by disruption in communication channels, supply chains and other network structures. Some authors (e.g. Milligan and Hutcheson, 2006) have attempted to identify the impact of information technology outsourcing on the organisation's resilience. It is worth noting that Milligan and Hutcheson (2006) distinguished the logical security risk among a number of other operational and maintenance risks. Despite the fact that such risks represent only a small part of the overall risks in the organisation, identification of the risks, and integrated risk management could be seen as a mature risk management approach. The organisational resilience from the business management system's perspective was analysed by Ignatiadis and Nandhakumar (2007). One of the key findings of the researchers is that complex business management systems, due to their own control mechanisms, often are very rigid in their nature, they have a tendency to reduce the overall levels of organisational flexibility and resilience. Some writers (eg. Werfs and Baxter, 2013) have been interested in resilience of socio-technical adaptive systems, however they do not emphasised the cyber threats as the main organisational stressors. In terms of the second iteration of resilience research, which was most intense at the beginning of the decade, it is worth noting that researchers mostly focused on development of resilience metrics and resilience

in critical infrastructure systems, management perspectives in the cyber resilience research of that time were extremely rare. One of the most notable is Goldman's (2010) work, where the author analysed a design of critical systems, deployment and management of processes from the perspective of resilience. One of the author's essential statements is a call to realise that it is not possible to stop cyber attacks, but the system's architecture reorganisation together with resilience approaches can reduce the consequences of the attack, raise their cost to the attacker and act as a deterrent in the future (Goldman, 2010). The cyber resilience has been explored not only as a system element but also as a design object (Bodeau et al., 2012; Bodeau, Graubart, Laderman, 2014; Häring, Ebenhöch, Stolz, 2016; Sansavini, 2017). There also are some attempts in the literature to explore the dynamics of the cyber resilience in different systemic environments, e.g. small business enterprises (Williams and Manheke, 2010), healthcare (Williams, 2010), cloud computing systems (Thebeau et al., 2014), e-health systems (Liveri, Sarri, Skouloudi, 2015), in the field of transportation (Nogal and O`Connor, 2017), electrical engineering (Zussblatt et al., 2017) in supply chains (Urciuoli, 2015), specific geographic and political units (Kaufmann, 2015; Peter, 2017), in the perspective of political complexity (Herrington and Aldrich, 2013), in the processes of preserving the reputation of the organisation (Wilding, 2016). It is also worth noting that significant number of different measurement modelling and metrics were designed, which can be used to measure the resistance of an organisation, system, department, or other organisational unit to cyber threats (Wang et al., 2010; Allen, 2011; Ford et al., 2012; Linkov and etc., 2013; Vugrin and Turgeon 2013; Houston and Sicker 2014; Bodeau and Graubart, 2016; Friedberg et al., 2016; Shapiro, 2016; Häring et al., 2017; Heinimann and Hatfield, 2017). One of the most notable models is created by Tran et al. (2016). The model is designed to overcome the challenges posed by zero-day malware. The phenomenon of cyber resilience in the critical infrastructure system's research has been seen as: a cornerstone element of national and corporate social responsibility (Ridley, 2011), the basis for complex critical infrastructure systems (Lewis, Mackin, Darken, 2011), critical infrastructure component from socio-political and procedural Perspectives (Lundborg and Vaughan-Williams, 2011; Moteff, 2012), as an element of industrial process control systems (Krotofil and Carden, 2013; Chaves et al., 2017), as the basis for critical infrastructure absorption, adaptation and recovery (Setola, Luiijf, Theocharidou, 2016; Balutis et al., 2016), as an element of social vulnerability of critical infrastructures (Trump et al., 2017), a critical element in the public-private partnership on critical infrastructure (Trucco and Petrnej, 2017), as a specific state of critical infrastructure (Todorovic and others, 2017). Due to the fragmentation and differences in the resilience perception, it is difficult to identify where the conceptual limits of one organisational cyber security management activity ends and where others start's. Such situation forms the demand to refine current terminology of cyber security concepts and to establish the conceptual limits of the use of each of these phenomena. Analysing the literature, legislation and statements of NATO an EU of top-level politicians, it can be argued that cyber resilience is one of the most of the necessary features of the socio-technical systems, but it is not clear how this property should be implemented, maintained and increased. Obviously, the principles of conceptual understanding and implementation of cyber resilience can be developed differently in different

socio-technical units by assessing the organisational culture and management traditions existing in a particular organisational space. **All the above statements can be summarised in the scientific problem expressed by the question**: how the cyber security management processes should be formed to increase organisations' resilience to the cyber threats?

Object of the research – improving of the cyber security management in organizations.

Purpose of the research – creation of a validated model of the organisational resilience to the cyber threats.

Goals of the research:

1. To perform literature analysis and to reveal the dynamics of cyber threats, the object of cyber security and cyber resilience, the cyber resilience management aspects, assumptions and obstacles of the cyber resilience formation, to identify key factors that determine the cyber security actualisation in the different levels of organisation management.
2. On the basis of theoretical insights, to form a conceptual organisational cyber resilience model, which integrates the most important organisational and systemic management factors.
3. To validate the conceptual organisational cyber resilience model and identify the key elements of its design by conducting the semi-structured expert interview and qualitative analysis of Lithuanian cyber security legislation.
4. To provide practical recommendations on how the cyber security management can be improved in organisations, using the cyber resilience approaches.

Defence statements

1. Cyber security research and practice domains are facing the issues related to lack of governmental aspects. Such situation requires clarification of terminology in the research area, harmonisation of concepts, the extension of the cyber security theory field with systemic and management perspectives.
2. Improvement of the cyber security management is inseparable from the growth of cyber security literacy levels of particular security community, capability of cyber security system's actors to exchange information, and promotion of inter-institutional cooperation at various levels of organisational system.
3. With the increase in the numbers of the cyber attacks and the level of their complexity, one of the most important features of the system becomes the cyber resilience, therefore the cyber security management based on the resilience approaches should be strongly encouraged. The cyber security management could be improved by applying the cyber security management model.
4. Development of the cyber resilience in organisations leads to the general evolution of the organisation, as a socio-technical system, and increases trust levels in the system by the system's users.

Methods of the research

Theoretical methods. In order to form theoretical basis of the organisation's model of cyber resilience, a scientific literature analysis was conducted, in which methods of systematisation, synthesis, comparison and generalisation were applied. Conceptual modelling and visualisation methods were used to formulate the model.

Empirical methods. Qualitative empirical research was used to validate the model. The methods used in the empirical research: expert interview, qualitative content analysis, analysis of secondary source data.

Scientific value and novelty of the dissertation. The study used an interdisciplinary, holistic approach to expand the existing discourse on cyber resilience research, including organisational and management aspects. The study clarified cyber resilience perceptions and outlined the main elements of cyber resilience in organisations. Organisational cyber resilience to cyber threats was analysed in the context of several management levels, thus creating conditions for further cyber resilience processes analysis. The research contributes to the overall field of cyber security research by creating the preconditions for further research of the resilience phenomenon.

Practical value of the research. The study reveals the existing cyber security management problems and proposes measures to address them using resilience-based approaches, thus improving cyber security management in public sector organisations in Lithuania. There is a growing number of calls to increase systems' resilience to the cyber threats, however there are practically no methodologies which describes how these processes should be implemented. The proposed cyber resilience model for organisations is applicable to the development of the cyber resilience initiatives in organisations at various levels of management.

Keywords: information security, cyber security, cyber security management, cyber resilience, cyber threats, resilience models for improving cyber security management.

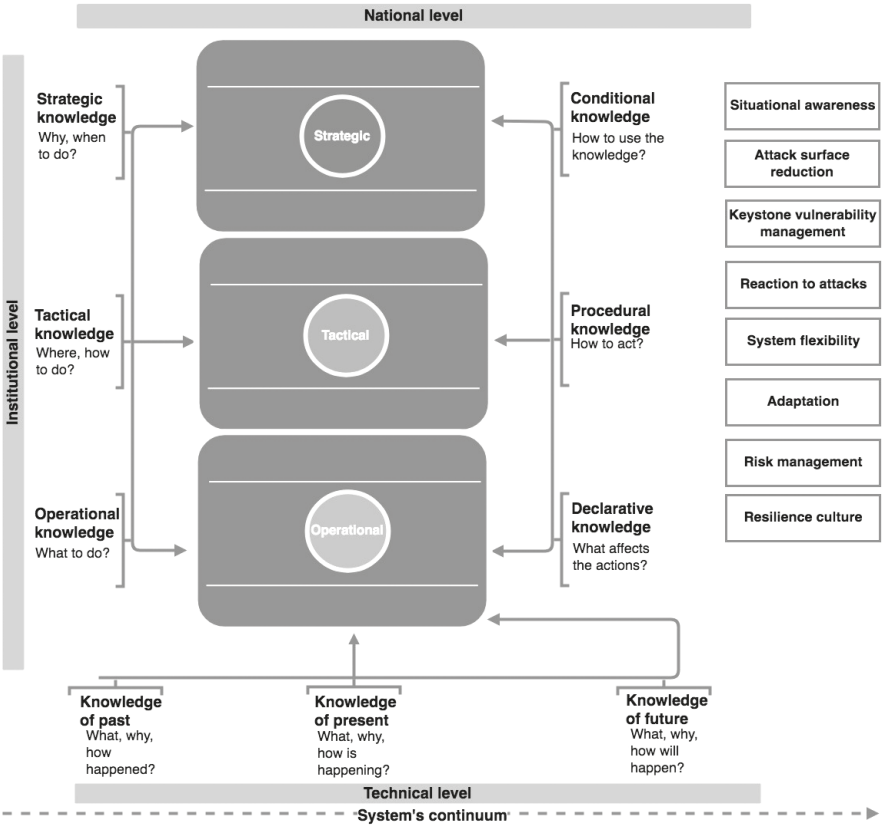
Source: *prepared by the author*

Figure 1. *Logical structure of the dissertation*

The first theoretical part of the dissertation covers the transformation of the cyber security phenomenon, reveals what caused the need for a conceptual rethinking of the information security and to search for the new ways to organize the cyber security activities. An overview of the dynamics of cybercrime threats, the evolution of cyber security management approaches and the need for new, resilient management approaches is provided. The second part of the dissertation describes the methodology used in the empirical research and in the analysis of the Lithuanian cyber security legislation. The final result

- the validated cyber resilience conceptual model, which integrates key elements of organisational cyber resilience, is provided in the third part of the dissertation.

Reviewed model of the cyber resilience. After conducting an expert interview, all the distinguished structural elements of the model were approved and can be considered as valid. A generalised conceptual model of cyber resilience is shown in Fig. 2.



Source: *prepared by the author*

Figure 2. *Reviewed model of the cyber resilience management*

The experts emphasised the need for communication across all vertical hierarchies of the organisation, therefore the cyber resilience model covers three organisational levels of cyber security awareness and collaboration: Strategic, Tactical, and Operational. None of state organisations performs its activities in a vacuum, it is affected by the general institutional system and processes in the whole national context. Organisations are using ICT to conduct their activities, and due to inadequate ICT usage, management and protection, there is a risk that the organisation's activities may be disturbed by the cyber

attacks. To address these issues, there are three additional levels distinguished in the model: Institutional, National, and Technological.

According to the experts, critical elements to increase the organisational resilience to the cyber threats are knowledge and communication. In order to maximise knowledge and communication between all the process participants, nine knowledge levels were developed:

- Organisation's hierarchical knowledge level:
  - Strategic knowledge level – at this level, knowledge is created; main questions answered: why particular cyber security activities are being carried out? Guidelines are set for the implementation of the activities.
  - Tactical knowledge level – awareness of the means by which strategic tasks should be carried out.
  - Operational knowledge level – knowledge of the implementation of specific actions.
- Organisation's analytical level of knowledge:
  - Knowledge of the past – knowledge of the past cyber threats, incidents, ways of eliminating them, digital forensics activities, post incident review, assessment of learnt lessons.
  - Knowledge of the present – monitoring, intrusion detection system information management, system anomaly analysis.
  - Future knowledge – forecasting, predictive data analysis, foresight.
- Organisation's meta-cognitive knowledge level (Schraw, 1998):
  - Conditional knowledge – knowing how to use the existing knowledge of the cyber security.
  - Procedural knowledge – knowing how to perform tasks from the cyber security perspectives.
  - Recognition knowledge – knowing how to increase the knowledge, what factors can influence formation of the knowledge.

When applying the model, each of its structural components (situational awareness, reduction of attack surface, etc.) must be assessed in the context of all the knowledge and activity levels.

Conclusions and recommendations

1st goal.

1. As the penetration of information and communication technologies in various fields of human activity is increasing constantly, the scale of the damage to organisations caused by the cyber attacks is raising accordingly. The impact of the threats affects not only virtual assets, but also the physical ones. Systems of public institutions, hospitals, the financial sector and the critical services are disrupted increasingly. This determines the need to evaluate cyber threats from a systematic perspective, and requires not only the shift in the perception of the security object from the narrow technological approach but also actualisation of the area at the level of national security.

2. There is a certain confusion of terminology in the discourse of cyber security - there are no sufficiently defined concepts. Together with terms that are specific to the early periods of the security, such as: information security, digital information security, the concepts which are more relevant for the current security periods (cyber security, cyber incident, etc.) are used. Therefore, the addition of new concepts to the existing terminology requires the definition and alignment of the existing terminology frameworks and the formulation of their conceptual links.
3. The development of perception of cyber security and resilience phenomena is developing together with cyber security literacy levels in a particular cyber security community. It is especially important that the concepts of cyber security, which are used in a particular cyber-security community are understood and interpreted in the same way by all members of the community. Before any categorisation of concepts, it is necessary to make sure that it will not adversely affect the objects of cyber security covered by these concepts, there will be no conceptual separation from the whole security terminology, which could cause negative consequences related to the financing of these objects, their development, and the perception of their overall importance.
4. The core of the cyber resilience management is a set of systemic factors, but adaptation, absorption and recovery capabilities are essential components which could prevent the movement of the system to an unwanted system configurations state when it is exposed to an external or internal stressor, a planned or unplanned change.
5. One of the main challenges in the development of the cyber resilience of organisational systems is the need to ensure the confidentiality of the system parameters and their governance measures, which results in information silos and information sharing distortions. Therefore, it is particularly important to ensure the proper communication between the management of the organisation and the units which are responsible for the cyber security.
6. Distribution of resources and prioritisation of activities have a direct impact on the cyber resilience and cyber security, and should therefore be assessed and developed in parallel with other processes of the organisational activities. They should be given the same level of priority when setting funding goals.
7. Dynamics of the resilience positively impacts the general processes of the organisation, contributes to the organisation's evolution. Appropriate and timely communication, inter-institutional cooperation, clear division of activities, avoidance of duplication are important to the organisational development. The diffusion of perception of the cyber resilience is also crucial, it should be performed by the vertical hierarchy of institutions from their top to the bottom. Implementation of the appropriate level of the cyber security measures in government's information systems increases citizens' confidence in the government.
8. In order to concretise the cyber security and resilience phenomena and to identify their conceptual boundaries, it is recommended to develop a discussion in this area among the cyber security experts representing different areas of expertise. In order

to identify future tendencies in the cyber resilience, trends in resilience development, transformation of cyber threats and to identify new models of resilience application, it is recommended to conduct continuous, interdisciplinary studies of the cyber resilience. It is recommended that one of the main directions of these research should be assessment of system's absorption capabilities.

2nd goal.

1. The concepts of organisational and system resilience are mobile, therefore most of the principles of resilience from one areas are applicable to the resilience models in other domains.
2. Despite the fact that lately information and communication technologies are widespread, there is a tendency towards the information silos, which isolates not only generic information flows but also the cyber security related information. Therefore, one of the most important tasks for organisations, which want to increase the levels of the cyber resilience, is to improve the cyber security situational awareness.
3. Identification of keystone vulnerabilities, which can cause danger to organisation's survival, and their proactive management, is a critical factor for ensuring proper continuity and crisis management.
4. One of the main components of the resilience is adaptability, which improves the organisation's ability to move from a reactive response to proactive readiness and ability to operate under conditions of high uncertainty.
5. System's flexibility is one of the determining factors in the formation of the system's resilience. It improves its ability to adapt to the cyber threats, transform its processes and systems according to the existing cyber security demand.
6. Taking into account the multifaceted nature of the cyber attacks, the reduction of the organisation's attack surface must be carried out in a complex way, integrating systemic and human factors.
7. In the context of intense convergence of socio-physical and technical systems, the improvement of the responses to attacks is a particularly relevant component of the systemic resilience.
8. The rising complexity of the cyber systems and their threats requires organisational and technical integration of the risk and resilience management processes.

3rd goal.

1. Initial components of the proposed cyber resilience model: Improvement of the cyber security situational awareness, improvement of keystone vulnerability management, improvement of adaptive skills, improvement of system flexibility, improvement of response to attacks, reduction of the organisation's attack surface, and improvement of the risk management are valid and relevant for development of the conceptual model of organisational cyber resilience management.
2. Improvement of the situational awareness should be accomplished through training of all staff members; the training should be based on practical examples of the cyber security.

3. In order to implement appropriate mechanisms for preparation to the cyber attacks, it is recommended to be aware not only about the current cyber security situation, but also to be able to anticipate potential cyber security threats in the future. For this purpose, it is necessary to develop cyber threat analysis mechanisms at the national level, which will help to predict potential threats and, taking into account the information received during the analysis, to proactively form the elements of cyber defence.
4. A particularly important factor for the cyber security situational awareness is the implementation of geopolitical situation evaluation mechanisms to monitor the geopolitical situation from the cyber security perspective. It is also necessary to carry out systematic monitoring of hackers, cybercriminals and their organisations.
5. In order to maximise the critical impact of keystone vulnerabilities management within an organisation, perception of critical vulnerabilities must be formed at the highest management level, with a clear positioning of keystone vulnerability management among all other necessary security elements.
6. In the whole range of essential measures for improving the keystone vulnerability management, it is recommended to emphasise training of employees, this would help to develop a cyber security culture of organisation, sector or state and to support proper cyber hygiene not only at the organisational level, but also at the level of the end user.
7. One of the main tools to improve the management of keystone vulnerabilities should be inventory and mapping of the assets in order to understand their links. The need to proper keystone vulnerability management is expressed best by explicitly showing the links with the assets and organisation's activities, and financial components.
8. The lack of keystone vulnerability management importance understanding can cause two main issues:
    - There is a probability not to get the approval to eliminate a vulnerability;
    - There is a probability of reverse manipulation, i.e. making of investments wherever they are not needed at all.
9. The keystone vulnerability management requires the achieving of consensus and common understanding of the current security situation by IT departments which administer the systems and the systems' owners; there is a need for a common understanding that the existing system vulnerabilities should be addressed before any system development activities and not vice versa. The development of security measures should be carried out, at least in parallel with the development of the systems.
10. Improvement of adaptation processes should start before crises or service level reductions in the organisation. Part of the adaptation mechanisms should be reflected in business continuity plans, with scenarios defining all possible actions for the crisis situations; it is necessary to improve the existing business continuity measures.
11. One of the most effective tools for improving adaptation are: exercises, including general system recovery and recovery from backup exercises. In order to increase the efficiency of the exercises, it is recommended to improve the exercising

mechanisms, thereby reducing internal resistance due to the time spent by staff and the additional exercise activities. When assessing the general tendencies of adaptation in Lithuania, it is worth noting that organisations have tendency to be more reactive than proactive or adaptive. This area should be improved together with post incident review activities.

12. An element, essential for ensuring the flexibility of a system is a human factor, so how much a person will remain rigid in his attitudes, intentions it will affect the rigidity levels of the system. A level of top management competency is very important to the system's flexibility, because the incompetent management may, for instance, order to use some existing components that may be completely inappropriate for improving the system's flexibility and resilience.
13. An attempt to achieve flexibility in the naturally static systems can produce negative results; therefore, for the systems to be flexible, it is recommended to build them from the scratch, otherwise the transition of the system from the rigid to the flexible state can be too complex.
14. Before deciding on the use of specific security measures, it is necessary to assess whether these measures are sufficiently effective to respond to existing security challenges, especially when cyber conflict evolves from a simple cyber incident to a systematic cyber warfare, and therefore there is a need to conceptually raise the importance of response actions to the level of cyber defence.
15. A critical components in the whole reaction to attacks process is a security policy and clearly defined response procedures.
16. Often too much attention is paid to reduce the organisation's attack surface from the perspective of external threats, however, one of the weakest and most vulnerable elements of the organisational system is the human factor and it is constantly underestimated.
17. With the growing numbers of social engineering attacks the training of employees becomes more and more crucial, which, together with the education about the cyber hygiene and procedural mechanisms should be one of the main security improvement measures. It is recommended to organise the training by allowing staff to actually participate in simulated attacks, subsequently showing the results and identified security gaps; such measures have the potential to be more effective in shaping the perception of the cyber security than the use of formal teaching methods.
18. Risk management is one of the main tasks in any organization, regardless of what type the risks are. IT risks are the part of all risks, so their management must be integrated into the organisation's risk management processes; an organisation with a high risk management culture is capable to manage all the risks in an integrated manner without diversifying them. Taking into account the tendency that IT issues are often ignored by other organisational units, it is necessary to form the cyber security culture in organisation and to improve the perception of the common cyber security issues. The perception of the issues increases the inertia of risk management and improves the general cyber security status in the organisation. The risk

management should exist in all system's lifecycle stages and should be implemented before any disturbing events, because the proper risk management could help organisation to return to its original state as fast as possible.

19. The risk management is directly related to the ability of different departments of a company, organisation or alliance to cooperate and to exchange information. This includes the dissemination of information, related to processes, work activities, equipment used, etc. If these processes are not carried out, members of the organisation do not understand the dangers properly. And if the dangers are not assessed adequately, it is difficult to define the risks that could occur in the organisation's systems, while the separate departments are performing activities, which are known only for the members of these departments. The more staff will know what processes are involved in specific organisational management activities, the better risk management will be. Therefore, one of the key tasks in the risk management is to involve as many people as possible from the different organisational sectors. The public sector in Lithuania has a tendency to delegate all risk management activities related to cyber security to IT departments. However, security and IT departments can provide only the necessary risk management tools, IT risk assessment should be performed by the organisational departments.
20. The risk management process in Lithuanian public sector are well regulated, but it is recommended to update methodological measures; the annual risk assessments are rather formal; not only security departments, should be involved in the overall risk management process. The extent of engagement is growing due to the understanding by managers that it is impossible for one person or a role, or a unit to conduct all the risk management activities.
21. Analysing the cyber security legislative acts, of Republic of Lithuania from the cyber resilience perspective, it is evident that the most comprehensively covered principles of the resilience are planning and preparation, however absorption and recovery dimensions are covered insufficiently. These findings support recommendations for future drafting of new legislation of the cyber security. It is recommended to take into account cognitive aspects of the resilience and all the resilience aspects of Absorption, Detection and Recovery phases.

Publications:

Grincevicius R. (2013). Mobile Government: Application, Development Factors and Future Perspectives. Social Technologies, 13, ISBN 978-9955-19-586-3.

Grincevicius R. (2012). Foresight As A Part of e-Government Strategic Planning Process: The Foresight Model. Social Technologies, ISSN 2029-7564, 2(1), p. 114–128.

Conferences:

Role of The Foresight in The e-Government Strategic Planning, Social Technologies, 2010.

Mobile Government: Application, Development Factors and Future Perspectives.

Projects:

Internationality in the Public Administration Studies

First name, last name: Rokas Grincevičius
Email: rokas.grincevicius@gmail.com

Education

2009-2011	Master in e-Government administration Mykolas Romeris University

Research interests: Information security management, cyber security, resilience, e-government

Work experience:

07/2018 – present	Senior technical consultant, European external action service/Fujitsu Belgium
08/2017 – 06/2018	Application responsible, COWI Lietuva, JSC
03/2016 – 07/2017	Platform engineer, Danske Bank, A/S Lithuania
12/2013 – 03/2016	Operations integration lead, Barclays Group Operations Limited
05/2013 – 12/2013	Senior IT specialist, Ministry of the Interior of the Republic of Lithuania
12/2010 – 06/2012	Lecturer, Mykolas Romeris University,
09/2007 – 12/2009	Database and information product manager Lintel, JSC (Telia group)
10/2005 – 09/2007	Project manager, Senukų prekybos centras, JSC, Vilnius

Grincevičius, Rokas
KIBERNETINIO SAUGUMO VALDYMO GERINIMAS TAIKANT ATSPARUMO MODELIUS ORGANIZACIJOSE: daktaro disertacija. – Vilnius: Mykolo Romerio universitetas, 2019. 224 p.

Bibliogr. 164–178 p.

ISBN (internete)
ISBN (spausdintas)

Nuolat dažnėja raginimai didinti sistemų atsparumą kibernetinėms grėsmėms, tačiau praktiškai nėra metodikų, aprašančių, kaip šie procesai turėtų būti įgyvendinami. Atsižvelgiant į tai, darbe išgrynintos kibernetinio atsparumo suvokties ribos, išskirti pagrindiniai organizacijų kibernetinio atsparumo elementai. Organizacijų atsparumas kibernetinėms grėsmėms išnagrinėtas keliais valdymo lygmenimis, taip sudarant prielaidas tolimesnei kibernetinio atsparumo procesų ir jų metu vykdomų sąveikų analizės plėtotei. Siekiant suformuoti kibernetinio saugumo valdymo modelio teorinį pagrindą buvo vykdoma mokslinės literatūros analizė, kurios metu taikyti sisteminimo, sintezės, lyginimo bei apibendrinimo metodai. Modelio suformavimui taikyti konceptualiojo modeliavimo ir vizualizacijos metodai. Modelio validacijai taikyti vienas kitą papildantys kokybiniai empiriniai tyrimai: ekspertinis interviu, kokybinė turinio analizė, antrinių šaltinių duomenų analizė.

There is a growing number of calls to increase systems' resilience to cyber threats, however there are no methodologies which describes how these processes should be implemented. Therefore the study clarified cyber resilience perceptions and outlined the main elements of cyber resilience in organisations. The organisational cyber resilience to cyber threats was analysed in the context of several management levels, thus creating conditions for further cyber resilience processes analysis. In order to form theoretical basis of the organisation's model of the cyber resilience, a scientific literature analysis was conducted, in which methods of systematisation, synthesis, comparison and generalisation were applied. Conceptual modelling and visualisation methods were used to formulate the model. Qualitative empirical research was used to validate the model. The methods used in the empirical research: expert interview, qualitative content analysis, analysis of secondary source data.

Rokas Grincevičius
KIBERNETINIO SAUGUMO VALDYMO GERINIMAS TAIKANT ATSPARUMO MODELIUS ORGANIZACIJOSE

Daktaro disertacija
Socialiniai mokslai, vadyba (03 S)

ISBN 978-9955-19-936-6 (internete)
ISBN 978-9955-19-937-3 (spausdintinis)

Mykolo Romerio universitetas
Ateities g. 20, Vilnius
Puslapis internete www.mruni.eu
El. paštas roffice@mruni.eu
Tiražas 20 egz. Užsakymo Nr. 21212

Parengė spaudai UAB „Baltic Printing House“
Svajonės g. 40, LT-94101, Klaipėda
www.balticprinting.com
Maketavo Laura Tekorienė

Spausdino UAB „Baltijos kopija“
Kareivių g, 13B, Vilnius
www.kopija.lt
El. paštas info@kopija.lt

ISBN 978-9955-19-936-6