MYKOLO ROMERIO UNIVERSITETAS

POLITIKOS IR VADYBOS FAKULTETAS

VADYBOS INSTITUTAS

JORDANA ŠABLINSKA

RIZIKOS SUVOKIMO ĮTAKA PASIRENGIMO VEIKTI EKSTREMALIOSIOSE SITUACIJOSE PROCESUI: INFORMACINIŲ TECHNOLOGIJŲ ORGANIZACIJOS TYRIMAS

Magistro baigiamasis darbas

Vadovė

prof. dr. B. Pitrėnaitė - Žilėnienė

VILNIUS, 2013

MYKOLO ROMERIO UNIVERSITETAS

POLITIKOS IR VADYBOS FAKULTETAS

VADYBOS INSTITUTAS

RIZIKOS SUVOKIMO ĮTAKA PASIRENGIMO VEIKTI EKSTREMALIOSIOSE SITUACIJOSE PROCESUI: INFORMACINIŲ TECHNOLOGIJŲ ORGANIZACIJOS TYRIMAS

Nepaprastųjų situacijų valdymo magistro baigiamasis darbas

Studijų programa 621N20023

Vadovė

_____ prof. dr. B. Pitrėnaitė - Žilėnienė

2013 11 17

Recenzentas

_____

2013

Atliko

NVSmns2-01 gr. stud.

_____ J. Šablinska

2013 11 15

VILNIUS, 2013

TURINYS

ĮVADAS 8
1. RIZIKA IR JOS SUVOKIMO TEORINIS INTERPRETAVIMAS 11
1.1. Rizikos samprata 11
1.2. Rizikos suvokimo aiškinimo kryptys 15
2. RIZIKOS SUVOKIMAS IR JO ĮTAKA EKSTREMALIŲJŲ SITUACIJŲ VALDYMUI 24
2.1. Rizikos suvokimo svarba besiruošiant ekstremaliosioms situacijoms 24
2.2. Pasiruošimo veikti ekstremaliosiose situacijose priemonės 28
2.2.1. Tęstinės veiklos plano rengimas 29
2.2.2. Pasiruošimo proceso mokymų organizavimas darbuotojams 36
2.2.3. Plano veiksmingumo patikrinimas 37
3. RIZIKOS SUVOKIMO ĮTAKA INFORMACINIŲ TECHNOLOGIJŲ ORGANIZACIJOS VEIKLAI 39
3.1. Tyrimo metodika ir organizavimas 39
3.2. Tyrimo rezultatų analizė 42
3.3. Tyrimo išvados 60
IŠVADOS IR REKOMENDACIJOS 62
LITERATŪRA 64
ANOTACIJA 71
ANOTATION 71
SANTRAUKA 72
SUMMARY 74
PRIEDAI 76

PRIEDAI

1 priedas. Žvalgomojo tyrimo klausimynas 77
2 priedas. Klausimynas apie rizikos suvokimą organizacijoje 78
3 priedas. Analitinių turinio vienetų išskyrimas 83
4 priedas. Žvalgomojo tyrimo respondentų atsakymai. 89
5 priedas. Grėsmių išskyrimo priežastys 94

LENTELĖS

1 lentelė. Rizikos suvokimo kategorijos 16
2 lentelė. Požiūris į organizacijos pažeidžiamumą..... 45
3 lentelė. Organizacijos pasiruošimas įveikti grėsmes..... 49
4 lentelė. Organizacijos apsaugos nuo grėsmių planas 52
5 lentelė. Savarankiško apsisaugojimo priežastys..... 56
6 lentelė. Priežastys lemiančios plano atsiradimą 58

PAVEIKSLAI

1 pav. Rizikos rūšys 12
2 pav. Rizikos suvokimo modeliai 17
3 pav. Atsparumo pavojingiems padariniams modelis 26
4 pav. Pasiruošimo ekstremaliosioms situacijoms procesas 29
5 pav. IT galimų grėsmių scenarijus 32
6 pav. Rizikos įgyvendinimo fazės 33
7 pav. Anketinės apklausos schema 40
8 pav. Klausimų analizės schema 42
9 pav. Respondentų darbo patirtis organizacijoje ir amžius 43
10 pav. Respondentų išsilavinimas 43
11 pav. Grėsmių išskyrimas 45
12 pav. Pažeidžiamiausios organizacijos sritys 48
14 pav. Mokymų, padėsiančių plėtoti organizacijos veiklą po ekstremaliosios situacijos, vykdymas 48
15 pav. Organizacijoje vykdoma rizikų analizė 51
16 pav. Reguliarus įrangos ir priemonių, skirtų apsisaugoti nuo grėsmių, atnaujinimas 51
17 pav. Pasiruošimo ekstremaliosioms situacijoms planas 52
18 pav. Plano skirto ekstremaliosioms situacijoms stokos priežastys 54
19 pav. Kitas planas, palengvinantis grįžimą prie įprastinės veiklos 54
20 pav. Už civilinę saugą atsakingo žmogaus buvimas 55
21 pav. Žinojimas kaip elgtis ekstremaliosios situacijos atveju esant darbo vietoje 55
22 pav. Dokumento, reglamentuojančio ekstremaliosios situacijos veiksmus, poreikis 58
23 pav. Informacija pateikta dokumente, reglamentuojančiame ekstremaliųjų situacijų veiksmus 60

SĄVOKOS

Ekstremalioji situacija – tai padėtis, kuri susidarė dėl ekstremaliojo įvykio ir gali sukelti didelį pavojų gyventojų gyvybei ar sveikatai, turtui, aplinkai arba gyventojų žūtį, sužalojimą ar padaryti kitą žalą.

Ekstremalusis įvykis – gamtinis, techninis, ekologinis ar socialinis įvykis, kuris kelia pavojų gyventojų gyvybei ar sveikatai, jų socialinėms sąlygoms, turtui ir (ar) aplinkai, atitinkantis, pasiekęs ar viršijęs nustatytus kriterijus.

Socialinis konstruktas – socialinis mechanizmas, fenomenas ar kategorija sukurta ir suformuota visuomenės. Kitaip tariant tai individo ar grupės suvokimas, kuris yra „sukonstruotas“ per kultūrinę ar socialinę praktiką.

Socialinis vienetas – organizacija laikoma didesnės socialinės grupės dalimi. Pvz., namų ūkiai, bendruomenės, verslas, viešosios ar valdymo institucijos.

ĮVADAS

Aktualumas ir naujumas. Dinamiška ir greitai besikeičianti aplinka įneša daug ir sunkiai nuspėjamų grėsmių, su kuriomis susiduria organizacijos. Nagrinėjamos temos svarba yra grindžiama tuo, kad rizikos suvokimas yra svarbus organizacijos veiklai spartėjančios globalizacijos laikais, kurie skatina naujų rizikų atsiradimą (Balžekienė, 2009), o organizacijoms yra svarbu užtikrinti savo nenutrūkstamą veiklą.

Daugėjant grėsmėms nėra imamasi joms įveikti skirtų pasiruošimo veiksmų, nes nėra suvokiama jų pasireiškimo rizika. Tai sukuria rimtą problemą, kadangi organizacija nesuvokianti galimo poveikio bus priversta nutraukti savo veiklą, nes nesugebės atsigauti po ekstremaliosios situacijos. Dėl šios priežasties organizacija, siekianti apsisaugoti nuo išorės neigiamų veiksnių privalo gebėti atpažinti rizikas, jas nuspėti ir valdyti. Tikėtina, kad organizacija, neįvertinusi rizikos arba perdėtai ją suvokianti gali nesugebėti prisitaikyti prie besikeičiančios aplinkos, todėl savo veikloje gali susidurti su minėtomis problemomis.

Besiruošiant ekstremaliajai situacijai yra susiduriama su dilema, kai reikia nuspręsti ar rizika iš tikrųjų egzistuoja, ir ar turės kokį nors poveikį organizacijos veiklai. Šios dvejonės atsiranda dėl skirtingų žmonių grupių skirtingai suvokiamos tos pačios rizikos (Sjoberg, 1999; Rimaitė, Rinkevičius, 2008). Skirtingas žmonių rizikos suvokimas lemia skirtingą elgesį toje pačioje situacijoje, kadangi individas gali neįvertinti ar pervertinti gresiančią riziką. Netinkamas rizikos suvokimas, jos neįvertinimas gali pakenkti organizacijai, nes nebus imtasi veiksmų, reikalingų atsiradusiai grėsmei pašalinti, o perdėtas rizikos suvokimas, jei rizika yra nedidelė arba jos išvis nėra taip pat kenkia organizacijos veiklai, nes žmogus gali imtis nereikalingų veiksmų nesančiai rizikai šalinti, be to bus išeikvoti turimi resursai. Vienas iš būdų galinčių išspręsti šią situaciją ir pagelbėti organizacijai atsigauti po ekstremaliosios situacijos yra pasiruošimas jai.

Nepaisant to, kad rizika ir jos suvokimas buvo nagrinėjami nuo senovės laikų, vis dėlto jos poveikis organizacijos elgsenai ekstremaliųjų situacijų metu buvo menkai ištirtas (Sjoberg, 2000). Daugiausia buvo orientuojamasi į pavienių asmenų ar bendruomenių rizikos suvokimą. Svarbu yra tai, kad rizikos suvokimas daro poveikį ne tik asmens elgesiui, sprendimų priėmimui ekstremaliųjų situacijų metu, bet taip pat pasiruošimui ekstremaliosioms situacijoms. Tik suvokus gresiančią rizika bus imtasi apsisaugojimo priemonių. Kadangi nuo rizikos suvokimo priklauso kaip organizacija gebės pasiruošti nenumatytiems atvejams, kokius pasiruošimo planus paruoš ir kaip apmokys darbuotojus elgtis nenumatytoje situacijoje, todėl darbe bus stengiamasi atskleisti gebėjimą pasiruošti ekstremaliosioms situacijoms informacinių technologijų (toliau - IT) organizacijoje per vyraujantį joje rizikos suvokimą.

Temos ištyrimo laipsnis. Rizikos suvokimo aiškinimus ekstremaliųjų situacijų metu daugiausia galima atrasti užsienio mokslininkų darbuose, Lietuvoje – ši tematika tyrinėta nedaug. Teorijos paaiškinančios įvairius požiūrius į rizikos suvokimą ir skirtingas rizikos suvokimo priežastis bei veiksnius atsispindi Lennarto Sjobergo (2000), Ortwin Renno (2004) ir Aistės Balžekienės (2009) darbe. Rizikos suvokimo svarba domėjosi Paulas Slovicius ir kt. (1982), o Aušros Rimaitės, Leonardo Rinkevičiaus (2008) darbe atsispindi sociokultūrinių veiksnių įtaka rizikos suvokimui Lietuvos mastu. Bendruomenių elgseną ir pažeidžiamumą ekstremaliųjų situacijų metu nagrinėjo Douglasas Patonas, Davidas Johnstonas (2001). Pasiruošimo ekstremaliosioms situacijoms aspektus tyrinėjo Kathleen J. Tierney (2001), Michael‘as K. Lindellis ir kt. (2006), Rolandas W. Perry‘s (2004) ir kt.

Tyrimo objektas – rizikos suvokimas.

Tyrimo dalykas – rizikos suvokimo įtaka organizacijos pasiruošimui veikti ekstremaliosiose situacijose.

Darbo problema – skirtingas rizikos suvokimas lemia nevienodą požiūrį į grėsmes. Nesuvokus galimos rizikos, tikėtina, kad nebus imtasi veiksmų, padėsiančių pasiruošti ekstremaliosioms situacijoms ir palengvinančių tolimesnės organizacijos veiklos vykdymą. Būtent todėl reikia spręsti klausimą, kokią įtaką rizikos suvokimas daro organizacijos pasiruošimo veikti ekstremaliųjų situacijų metu procesui?

Darbe buvo iškeltos trys **hipotezės**:

H_1: IT organizacijos darbuotojai kaip didžiausią poveikį turinčias organizacijos veiklai išskiria technologines grėsmes.

H_2: tiriama organizacija neturi plano aprašančio pasiruošimo veiksmus ekstremaliosioms situacijoms.

H_3: respondentai neįžvelgia tęstinės veiklos plano poreikio savo organizacijai.

Darbo tikslas – išanalizuoti ir įvertinti ar bei kokią įtaką daro rizikos suvokimas pasiruošimui ekstremaliosioms situacijoms.

Uždaviniai:

1. Išanalizuoti rizikos suvokimo teorines įžvalgas ir jo svarbą ekstremaliosiose situacijose.
2. Nustatyti ir analizuoti priemones, kurios padėtų didinti suvokimą ir tobulinti pasiruošimą ekstremaliosioms situacijoms.
3. Nustatyti ir įvertinti rizikos suvokimo lygį ir pasirengimo veikti ekstremaliosioms situacijoms priemones organizacijoje.
4. Pateikti tyrimo išvadas ir rekomendacijas, padėsiančias gerinti rizikos suvokimą organizacijoje.

Tyrimo metodai: darbe atlikta mokslinės literatūros, kiekybinė ir kokybinė duomenų analizė. Gautų kiekybinių duomenų apdorojimui buvo atlikta statistinė analizė, o kokybinių – turinio analizė.

Siekiant išsiaiškinti, kaip IT organizacijoje vyraujantis rizikos suvokimas lemia jos pasiruošimą veikti ekstremaliųjų situacijų metu, buvo pasirinktas vienas iš kiekybinio tyrimo metodų – anketinė apklausa.

Darbo struktūra. Pirmoje darbo dalyje „Rizika ir jos suvokimo teorinis interpretavimas“ yra aptariama rizikos samprata, jos suvokimo kitimas, o taip pat nagrinėjamas rizikos suvokimas vadovaujantis keturiais požiūriais. Antroje dalyje „Rizikos suvokimas ir jo įtaka ekstremaliųjų situacijų valdymui“ yra gvildenamas rizikos suvokimo ir pasiruošimo ekstremaliosioms situacijoms santykis, nagrinėjama rizikos suvokimo svarba ekstremaliosioms situacijoms. Plačiau apžvelgiamas pasiruošimo ekstremaliosioms situacijoms planų kūrimas, jų svarba bei planų tinkamumo patikrinimas. „Rizikos suvokimo įtaka informacinių technologijų organizacijos veiklai“ yra trečia darbo dalis, kurioje yra pristatomas atliktas tyrimas, atskleidžiantis kaip rizikos suvokimas lemia organizacijos pasiruošimą veikti ekstremaliosiose situacijose.

1. RIZIKA IR JOS SUVOKIMO TEORINIS INTERPRETAVIMAS

1.1. Rizikos samprata

Ateities įvykiai gali būti sunkiai nuspėjami, todėl imantis tam tikrų veiksmų mes rizikuojame. Stengiantis apsisaugoti nuo rizikos poveikio reikėtų imtis priemonių jai sumažinti. Siekiant nustatyti rizikos suvokimo poveikį organizacijos veiklai ir ją valdyti pirmiausia svarbu išsiaiškinti, kokia reikšmė yra priskiriama rizikai, kaip ji yra suvokiama ir kaip jos suvokimo pokyčiai susiję su organizacijos galimybėmis veikti ekstremaliųjų situacijų metu.

Rizikų masto augimas parodo, kad žmonija geba keisti savo aplinką, ji pati sukuria ir sumažina rizikas (Slovic, 1987). Dėl vykstančių pokyčių keičiasi ne tik rizikos atsiradimo mastai, bet taip pat jai priskiriama reikšmė. Rizikai skirtingą reikšmę suteikia individai, jų grupės ir organizacijos. Kiekviena darbo ar mokslo sritis taip pat sukuria skirtingą reikšmę rizikai. Siekiant suprasti, ką reiškia žodis rizika svarbu išnagrinėti įvairias jai priskiriamas sampratas ir išsiaiškinti, kokie yra esminiai šių rizikai suteikiamų reikšmių skirtumai.

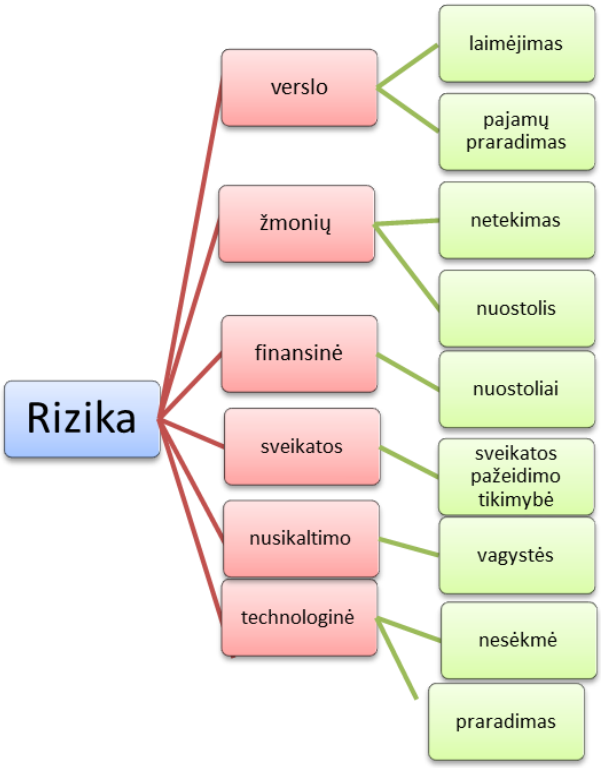
Žodžiui *rizika* kiekvienu laikmečiu buvo suteikiama skirtinga reikšmė. Tai lėmė naujų ir greičiau atsirandančių grėsmių tendencijos.

Pirmą kartą rizikos samprata buvo pavartota vakarų keliautojų ir buvo siejama su galimais pavojais plaukiojant jūroje. Ji buvo suprantama kaip natūralus dalykas ir pabrėžtina, kad žmogiškojo faktoriaus, t.y. žmogaus atsakomybės ir kaltės, neįtraukė. O aštuonioliktajame amžiuje rizikos samprata buvo sumokslinta ir siejama su tikimybe (Lupton, 1999a).

Rizikos apibrėžimas buvo plečiamas ir apėmė naujus veiksnius, t.y. ji buvo tapatinama ne vien tik su gamtos įvykiais, bet taip pat buvo įtrauktas ir žmogiškasis veiksnys. Tai lėmė, kad rizikos galėjo būti sukeltos žmogaus, o ne tik vertinamos kaip lemtis (Lupton, Tulloch, 2002). Vėliau rizika buvo vartojama įvairiose srityse, kaip antai, verslo pasaulyje ir buvo tapatinama su laikinumu. Laikui bėgant samprata išsiplėtė iki neapibrėžtumo (Lupton, 1999a; Denney, 2005). Rizika buvo laikoma neutraliu terminu susijusiu su tikimybe, netektimi ar laimėjimu, o prasidėjus moderniesiems laikams rizika buvo suvokiama kaip neigiama ir nepageidaujama (Fox, cit.pgl. Lupton, 1999b). Ji buvo tapatinama su kažkuo nežinomu, keliančiu baimę, nevaldomu, neteisingu, katastrofišku, netikėtu bei galinčiu paveikti ateities kartas (Slovic ir kt., 1982; Crouhy, 2006). Remiantis pateiktais kintančiais rizikos apibūdinimais galima teigti, kad rizika yra kažkas neapčiuopiamo.

Nuo rizikos sampratos vartojimo jūreivystėje buvo pereita prie rizikos versle, kasdienėje veikloje, o taip pat tokiose srityse kaip finansai, ekonomika, sveikata ir daugybėje kitų sričių, todėl ji yra apibrėžiama ne vienodai. Yra išskiriama daugybė šių sričių rizikų (1 pav.). Nors kiekvienoje srityje

rizika yra apibrėžiama skirtingai, bet tuo pačiu esminiai rizikos ypatumai, tokie kaip neapibrėžtumas, netikėtumas, nuostoliai ir kt., išlieka.



1 pav. **Rizikos rūšys**
Šaltinis: sudaryta pagal Sweeting, 2011, p. 93-104; Janušonis, 2005, p.23; Davidson, 2003, p.10

Finansų srityje yra išskiriama nemažai rizikos rūšių, t.y. rinkos rizika, kredito rizika, likvidumo rizika, veiklos *(angl. operational)* rizika. Taip pat su finansais siejama sisteminė rizika, palūkanų normos rizika ir kitos. Kaip pavyzdį galima pateikti vieną iš finansinių rizikų rūšies, t.y. likvidumo rizika, kuri yra apibrėžiama kaip *nuostoliai*, kurie atsiranda dėl nesugebėjimo padengti verslo ar prekybos išlaidų (Satyajit, 2006; Sweeting, 2011). Šioje srityje į riziką yra žvelgiamą kaip į neigiamą, nuostolingą dalyką. Nagrinėjant finansines rizikas yra orientuojamasi į tai, kad jos yra susijusios su galimais nuostoliais.

Autoriai Vinsas Janušonis (2005) ir Romanas Urniežius (2001) pateikia iš pirmo žvilgsnio panašius rizikos apibrėžimus, tačiau juose galima įžvelgti autorių besiskiriančias pozicijas. V. Janušonis (2005) riziką įvardija kaip veiksmą, kuriam mes pasiryžtame, nes numatome, kad galime pasiekti tikslą arba tai pasiryžimas nesiimti veiksmų, padėsiančių pašalinti neigiamus padarinius, nes tikima, kad bus išvengta neigiamų padarinių. O kalbėdamas apie sveikatą autorius rizikos sąvoką susiaurina. Sveikatos srityje rizika yra tapatinama su paciento sveikata arba kaip V. Janušonis (2005)

įvardija „paciento sveikatos pažeidimo tikimybė“ (p. 23). R. Urniežius (2001) pateikia iš pirmo žvilgsnio beveik identišką V. Janušoniui rizikos sampratą, tačiau autorius numato galimybę imtis veiksmų, įvertinant, kad tikslas gali būti nepasiektas, anot jo, rizika tai „ryžtas veikti žinant, kad galima tikslo ir nepasiekti“ (p. 7). Šiame apibrėžime pastebimas *praradimas* patirtas nepasiekus užsibrėžtų tikslų. Nepaisant to, kad abu autoriai pateikia atrodytų panašius rizikos apibūdinimus, vis dėlto galima išskirti du požiūrius į riziką, pirmuoju atveju tikima laimėjimu ir į riziką yra žvelgiama teigiamai, išskyrus autoriaus pateiktą rizikos suvokimą sveikatos srityje, antruoju – imamasi veiksmų įvertinant pralaimėjimą ir atskleidžiamas neigiamas požiūris.

Priešingai nei jau išvardintose srityse, versle rizika yra suprantama kaip iššūkis, kurį reikia priimti siekiant įgyvendinti organizacijos tikslus (Steinberg, 2011). Šiuo atveju yra pastebimas teigiamas, pažangą skatinantis požiūris į riziką. Kadangi versle yra orientuojamasi į užsibrėžtą tikslą, todėl tai kas trukdo jį pasiekti yra suvokiama kaip rizika.

Be jau paminėtų rizikų tenka susidurti nusikaltimo, žmonių, projektų, duomenų, strateginėmis, gero vardo, teisinėmis, reguliuojamosiomis rizikomis. Visos šios rizikos orientuojasi į neigiamą požiūrį, pvz., esant rizikai, kad organizacija įdarbina netinkamus darbuotojus vyrauja žmonių rizika, o susiduriant su vagystėmis ar kitais nusikaltimais pasireiškia nusikaltimo rizika. Yra atrandama skirtingos rizikos klasifikacijos, viena vertus rizika gali būti laikoma atskira atšaka, kita vertus – ji galinti daryti poveikį kitai rizikai ir būti jos poskyriu (Davidson Frame, 2003).

Sudėtinga tiksliai apibrėžti kiek ir kokių rizikų yra, tačiau viena yra aišku – kiekvienoje srityje yra susiduriama su tam tikromis rizikomis. Ne tik atsiranda naujų, bet ir esamos nuolat plečiasi. Netgi įvardijus gresiančias rizikas reikėtų nuolat gilintis į naujo pobūdžio rizikas, nes kaip teigia Paulas Sweetingas (2011), „laikui bėgant vystysis naujos rizikos“ (p. 93). Jos yra skirtingos, tačiau nepaisant to, didžioji dalis rizikų atneša nuostolius ir nepageidautinus padarinius, kurie neigiamai atsiliepia organizacijos veiklai.

Nagrinėjant rizikos sampratas, kurios nėra siejamos su kažkuria konkrečia sritimi taip pat pastebima, kad dažniau rizika yra suprantama kaip neigiamas nei teigiamas dalykas. Rizika yra apibrėžiama kaip tikimybė, kad tam tikrą akimirką gali įvykti kažkas nepageidautino, nenumatyto, blogo bei sukeliančio neigiamus padarinius (Merna, Al – Thani, 2008). Dėl šios priežasties ji asocijuojasi su praradimais, nuostoliais, nepasiektais tikslais.

Anot Paulo Hopkino (2010), rizika gali atspindėti teigiamus arba neigiamus rezultatus, arba sukelti neapibrėžtumą, o Julia Rutherford (2008) papildė, jog tai yra kažkas nežinomo. Todėl rizika yra siejama su galimybe arba netektimi, praradimais, arba neapibrėžtumo pasireiškimu organizacijoje. Atsižvelgiant į tai, kad autorė riziką susiejo ne tik su neigiamomis pasekmėmis, bet ir su galimybe, parodo, jog rizikos sampratoje ji neįžvelgia vien tik neigiamų dalykų. Apibendrinant pateiktas rizikos sampratas galima pasinaudoti Michael‘o Blytho (2008) apibrėžimu. Jis supaprastintai, pateikia

formulės pavidalo rizikos sampratą, anot autoriaus, riziką galima pavaizduoti kaip įvykio tikimybės ir padarinių po įvykio santykį. Kitaip tariant, jis išskiria du veiksnius, kuriais apibūdina riziką, t.y. tikimybę ir padarinius.

Taip pat pastebimas rizikos tapatinimas su tikslais ir įvykiais. Rima Tamošiūnienė, Olga Savčiuk (2007) riziką tapatina su kylančia grėsme organizacijai, kadangi dėl rizikos organizacija susiduria su neigiamomis aplinkybėmis, kurios trukdo jai pasiekti nusistatytų tikslų (p. 204). Kaip teigia autorės, tikslai tai pagrindinis aspektas, kuriam nesant nebūtų rizikos. Tačiau P. Hopkinas (2010) laikosi priešingos nuomonės. Anot jo, nėra tikslinga riziką sieti su organizacijos tikslais, kurie dažnai nėra rutininiai, besitęsiantys organizacijos tikslai, o greičiau tokie, kurie sąlygoja pokyčius. Todėl, pasak autoriaus, geriausiai rizika apibūdinama ją tapatinant su tam tikru įvykiu ar įvykiais. Tai yra paaiškinama tuo, kad nesant įvykio nebus rizikos.

Manytina, kad geriausiai šias skirtingas pozicijas apibendrina Georges Selimo, Davido McNamee (1999) pateiktas rizikos apibūdinimas, kuriame autoriai rizika sieja tiek su tikslais, tiek su įvykiais. „Rizika tai idėja skirta išreikšti neapibrėžtumą dėl įvykių ir/ar jų rezultato, kuris gali turėti svarbų poveikį organizacijos uždaviniams ir tikslams“ (p. 163). Kaip ir pirmuoju atveju remiantis pateiktu rizikos apibrėžimu yra aiškiai išryškinama konkreti rizikos grėsmė, t.y. organizacijos tikslai, kurie paveikti rizikos negalės būti įgyvendinti. Tačiau tai atsitiks tik tuo atveju, jei atsitikęs įvykis turės poveikio tikslams. Būtent todėl organizacijai, siekiančiai apsaugoti savo interesus, yra itin svarbu įvertinti kylančias grėsmes.

Nepaisant visuomenėje labiau paplitusio negatyvaus požiūrio į riziką, taip pat yra manoma, kad ji atspindi ir teigiamus dalykus. Teigiamo požiūrio šalininkų manymu, rizika suteikia akstino veikti, nes yra kaip „teigiama jėga skatinanti siekti gerų dalykų, dalyvauti kuriant pažangią visuomenę“ (Denney, 2005, p. 11), būtent rizika suteikia galimybę tobulėti. Autorius kaip ir anksčiau minėta J. Rutherford (2008) taip pat įžvelgia galimybes, kurias gali suteikti rizika.

J. Davidsono Frame (2003) kaip ir O. Renno (1998) nuomone, rizikai apibrėžimą suteikia pats žmogus priklausomai nuo jo paties požiūrio. O kadangi tuo pačiu klausimų žmonės gali turėti skirtingą požiūrį, todėl rizika gali turėti ne vieną apibrėžimą. Didžioji dalis anksčiau pateiktų rizikos apibrėžimų yra gana abstrakti, kadangi sunku apibrėžti kas yra *neigiama, bloga arba gera*. Tai kas vienam gali atrodyti kaip neigiamas dalykas, kitam įprasta situacija. Rizikos sąvokų apibūdinime ypač nagrinėjant teigiamus ar neigiamus aspektus atsispindi subjektyvus rizikos interpretavimas, t.y. jos suvokimas.

Tikimybė nepasiekti numatyto tikslo yra suprantama kaip rizika. Modernėjant pasauliui kito rizikos reikšmės, kurios vėliau buvo priimamos ne tik kaip likimas ar natūralus įvykis, bet ir kaip žmogiškojo faktoriaus įsikišimo pasekmė. Atsirandančios naujos grėsmės lėmė vis dažnesnį rizikos įraukimą į kasdienį žmonių kasdienį gyvenimą, verslą, finansus, technologijas ir daugelį kitų sričių,

kuriose jai suteikiama reikšmė šiek tiek skyrėsi. Tačiau nepaisant skirtingos reikšmės priskiriamos rizikai, ji buvo tapatinama daugiau su neigiamais nei teigiamais rezultatais, padariniais ir tikimybe.

1.2. Rizikos suvokimo aiškinimo kryptys

Rizikai priskiriama reikšmė yra ne ką svarbesnė nei tai, kaip yra suvokiama rizika. Suvokus galimą riziką įmanoma tinkamai, realistiškai įvertinti gresiančią ekstremaliąją situaciją ir imtis tinkamo elgesio. Rizikos suvokimas numato asmens poveikį veikti ir susidoroti su gresiančia situacija bei daro įtaką jo elgesiui ekstremaliosios ar bet kurios kitos situacijos metu. Todėl svarbu išsiaiškinti veiksnius ir požiūrius, lemiančius nevienodą rizikos suvokimą.

Mokslininkai (Sjoberg, 1999; Paton, Johnston, 2001; Renn, 2004; Balžekienė, 2009) tyrinėję rizikos sritį priėjo prie išvadų, kad žmonės skirtingai suvokia riziką. Skirtingas žmonių rizikos suvokimas lemia jų skirtingą gebėjimą veikti ekstremaliosiose situacijose. Vieni žmonės perdėtai suvokia riziką, kiti – neįvertina artėjančių grėsmių. Berndas Rohrmannas (2008) teigia, kad yra žmonių, kurie nuolat įžvelgia riziką, net jei ji jiems negresia. Dėl suvokime pasireiškiančių skirtumų rizikos suvokimas yra ypač svarbus tiems, kurie atsakingi už saugumą, todėl jie privalo žinoti, kaip visuomenė reaguoja į rizikas (Slovic, 1987). Žinojimas padės imtis tinkamų priemonių apsisaugant nuo kylančių grėsmių ir laiku perspėjant žmones.

Siekiant nustatyti kylančią tam tikrų įvykių riziką yra išskiriami du blokai, atvaizduojantys, kaip yra vertinama rizika. Pirmuoju atveju, rizika yra nustatoma remiantis moksliniais apskaičiavimais. Antruoju – yra vertinama subjektyviai, remiantis įvairiais, nepamatuojamais veiksniais, tokiais kaip, patirtis, informatyvumas, sociokultūriniai aspektai ir kt.

Šios įvardintos rizikos yra vadinamos objektyviąja ir subjektyviąja rizika. Objektyvioji nuo subjektyviosios skiriasi tuo, kad pastaroji yra paremta asmens proto būsena, t.y. paties asmens nuomonė, jo suvokimas apie riziką. Rizika prasideda žmogaus galvoje ir atspindi asmens patyrimą, stebimą aplinką, jo įsitikinimus ir nuostatas bei stereotipus (Taylor – Gooby, Zinn, 2006; Rejda, 2008; Renn, 2008; Garcia de Castillo, 2012). Būtent todėl, šis procesas paremtas individualiais ir skirtingais veiksniais yra vadinamas suvokiama rizika. Objektyvioji rizika tai skirtumas tarp tikrojo ir tikėtino nuostolio. Šios rūšies rizika priešingai nei subjektyvioji yra pamatuojama, apskaičiuojama, todėl ji dažniausiai yra taikoma ekspertų (Rejda, 2008).

Subjektyvi rizika pasižymi tuo, kad remiantis ta pačia rizika vyrauja skirtingas jos suvokimas ir elgesys. Aukšto lygmens subjektyvi rizika sąlygoja apdairų elgesį, kai tuo tarpu, žemo lygmens subjektyvi rizika skatina mažiau atsargų elgesį (Rejda, 2008). Skirtingas rizikos suvokimas yra aiškinamas tuo, kad žmogus negalėdamas apsisaugoti nuo rizikų pats pasirenka, kas jam kelia grėsmę, ką laikyti rizika bei nuo ko reikėtų saugotis. Manymas, kad riziką galima kontroliuoti sąlygoja žemą

rizikos suvokimą (Renn, 2008). Vyraujantis suvokimas skatina imtis įvairių, kartais netinkamų saugumo priemonių.

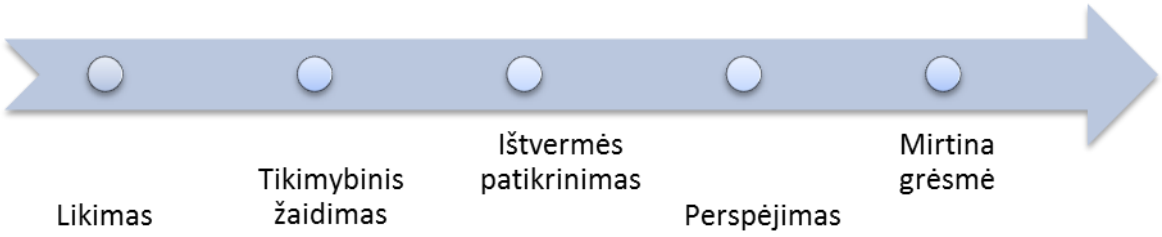
Rizikos suvokimą nulemia žmonių požiūris, elgesys, patirtis, tikėjimas, aplinka, kurioje jie randasi ir daugelis kitų veiksnių. Aiškinant rizikos suvokimą galima išskirti tris kategorijas (1 lent.), kurios pateikia rizikos suvokimo aspektus. Rizikos suvokimas yra aiškinamas pagal rizikai priskiriamą žmonių reikšmę, pagal veikėjus arba kitaip pagal ją interpretuojančius subjektus ir skirtingas pozicijas aiškinančias teorijas.

1 lentelė. Rizikos suvokimo kategorijos

<table>
<tr><th colspan="6">Rizikos suvokimas</th></tr>
<tr><td colspan="2">Veikėjai</td><td colspan="2">Priskiriama reikšmė</td><td colspan="2">Aiškinimo sritis</td></tr>
<tr><td rowspan="3">Ekspertai</td><td rowspan="3">Visuomenė (ne specialistai)</td><td>Likimas</td><td>Ištvermė</td><td rowspan="2">Kultūrinė</td><td rowspan="2">Socialinė</td></tr>
<tr><td>Grėsmė</td><td rowspan="2">Perspėjimo rodiklis</td></tr>
<tr><td>Žaidimas</td><td>Psichologinė</td><td>Politinė</td></tr>
</table>

Dažniausiai rizikos suvokimas yra aiškinamas išskiriant įvairius anksčiau paminėtus veiksnius, o teorijos sugrupuoja ir nagrinėja suvokimą platesniu aspektu.

Siekiant išsiaiškinti, kas sąlygoja skirtingą rizikos suvokimą pagal jai priskiriamą reikšmę, buvo nagrinėjami įvairūs veiksniai. Nagrinėjant technologines ir natūralias grėsmes, yra išskiriamos penkios rizikos suvokimo grupės arba rizikos suvokimo modeliai, t.y. rizika yra suvokiama kaip mirtina grėsmė, kaip likimas, ištvermės patikrinimas, tikimybinis žaidimas ir išankstinis perspėjimo rodiklis (Renn, 2004). Tuo yra parodoma, kad kiekvienas žmogus riziką suvokia ir interpretuoja savaip, priklausomai nuo turimos informacijos bei patirtų išgyvenimų, todėl rizikos suvokimas ir yra laikomas subjektyviu. Šį paaiškinimą galima pavaizduoti tiesėje pagal pavojingumą, t.y. nuo visiško rizikų ignoravimo iki susirūpinimo jomis (2 pav.).



2 pav. **Rizikos suvokimo modeliai**

Remiantis pirmu modeliu, jei žmogus riziką suvokia *kaip likimą* (Renn, 2004) arba kitaip kaip *Dievo veiksmus* (Borodzicz, 2005), pvz. žemės drebėjimą, potvynį, vadinasi, jis gali nesiimti jokių veiksmų, padėsiančių susidoroti su gresiančia ar įvykusia ekstremaliąja situacija, nes tikės, kad tas įvykis nepriklauso nuo jo. Priešingai nei suvokimas, kad rizika yra mirtina grėsmė, šiuo atveju žmonės yra linkę neigti, kad retai įvyksiantis pavojus yra ar gali atsirasti ir linkę pabėgti, kai tam tikras įvykis atsitinka dažnai.

Kai žmonės yra linkę nepakankami įvertinti reto įvykio tikimybės, vadinasi, jie riziką suvokia kaip *tikimybinį žaidimą*. Tikimybinio žaidimo procesas yra orientuotas į laimėjimą ar pralaimėjimą, kurie nepriklauso nuo žaidėjo gebėjimų (Renn, 1998; 2004).

Žmonės rizikuoja su tikslu *patikrinti savo ištvermę* ir patirti laimėjimą susiduriant su rizikos faktoriais. Tačiau rizika su kuria yra susiduriama yra netikra, o imituota, t.y. atliekami simuliaciniai žaidimai, spėjimai investicijų srityje, sportas. Kadangi reali rizika yra paverčiama dirbtine, netikra, todėl vis labiau tikima, kad bus išvengta susidūrimo su realia rizika, tikima, kad pasirinkti veiksmai yra kontroliuojami (Renn, 1998; 2004). Dėl šios priežasties sumažėja realios rizikos objektyvus įvertinimas, nes apskritai abejojama, ar reali rizika egzistuoja.

Nors šie du pastarieji rizikos suvokimo modeliai atrodo panašūs, tačiau taip nėra. Abiem atvejais yra rizikuojama, tik pirmuoju atveju, t.y. suvokiant riziką kaip tikimybinį žaidimą, yra koncentruojamasi į galimybę laimėti, t.y. į galutinį rezultatą, o ne į procesą, o antruoju – dėmesys yra skiriamas pačiam procesui apeinant rizikos galimybę.

Rizika taip pat yra suvokiama kaip *išankstinis perspėjimo rodiklis*. Šis suvokimas remiasi priežasčių, sukėlusių tam tikrus padarinius, paieška. Jis padeda aptikti pasislėpusį pavojų ir tarsi perspėja, jog reikėtų atkreipti dėmesį į tam tikrus dalykus. Tai yra daroma nustatant ryšį tarp veiksmų ir užslėptų padarinių (Renn, 2004). Pastebėtina tai, kad žinios apie grėsmės riziką yra paremtos ne asmenine patirtimi, o informacija gauta iš aplinkinių. Dėl šios priežasties, jei pateikta informacija neatitiks galimos rizikos, pasitikėjimas informacijos šaltiniu sumažės (Renn, 1998).

Paskutinis rizikos suvokimo modelis, kuris remiasi tuo, kad *rizika yra mirtina, lemtinga (angl. fatal) grėsmė*, atsirandanti iš baimės dėl nežinomų dalykų, teigia, kad grėsmingas įvykis gali atsitikti bet kada. Žmonės yra labiau įbauginti tų įvykių, kurių negali nuspėti ir jiems pasiruošti. Nuspėti retų atsitiktinių įvykių yra praktiškai neįmanoma, todėl dėl jų yra baiminamasi labiau. Įvykstanti nuosekli grandinė reguliarių įvykių leidžia pasiruošti gresiantiems pavojams ir kontroliuoti riziką (Renn, 2004).

Šie įvairūs požiūriai, atskleidžiantys rizikos suvokimą, patvirtina, kad į riziką yra žvelgiama iš daugiamatės pozicijos. O jai priskiriama reikšmė priklauso nuo konteksto kuriame yra analizuojama.

Bandant įvertinti skirtingai suvokiamą riziką yra nagrinėjami ne tik individų suvokimą lemiantys veiksniai, bet ir žvelgiama į skirtingus ją atspindinčius tam tikrų autorių požiūrius. Vertinant riziką kultūriniu - antropologiniu, socialiniu, psichologiniu ir politiniu aspektais yra išskiriamos keturios teorijos, paaiškinančios kaip yra interpretuojamas rizikos suvokimas iš skirtingų pozicijų.

Kultūrinis – antropologinis požiūris pateikia **kultūrinę teoriją**, kuria remiantis rizikos suvokimas yra paremtas kultūra. Remiantis kultūrine teorija yra apibrėžiamos kultūrinės ribos tarp individų, bendruomenės socialinių grupių ir tarp bendruomenių. Veiksniai ar rizikingos grupės, keliančios grėsmę socialinei tvarkai ir galintys sukelti pavojų, yra laikomi rizika. Teigtina, kad pagal šią teoriją individo rizikos suvokimas yra išreiškiamas priklausomai nuo kultūrinio suvokimo, vyraujančio toje aplinkoje, kurioje jis randasi. Todėl tik „perfiltruotas“ per bendruomenės / kultūros prizmę rizikos suvokimas formuoja individo suvokimą (Lupton, 1999b).

Rizikos socialinis konstruktas yra susijęs su žmonių tarpusavio kasdiene sąveika (Borodzicz, 2005; Taylor – Gooby, Zinn, 2006). Vadinasi, individo rizikos suvokimas yra formuojamas priklausomai nuo aplinkos, kurioje gyvena ir priklausymo tam tikrai grupei, kaip antai, šeimai, draugų ratui ar kt. Darytinos prielaidos, kad ta aplinka, kurioje asmuo randasi veikia individo rizikos suvokimą, todėl toks suvokimas gali būti subjektyvus, nes yra pagrįstas ne realiu ar individualiu suvokimu, bet greičiau poveikiu iš šalies.

Kita teorija, siekianti išaiškinti rizikos suvokimą, yra **rizikos visuomenės** teorija, kuri yra analizuojama socialiniu požiūriu. Ši teorija įtvirtino supratimą, kad rizikas reikėtų vertinti ne kaip lemtį, tačiau kaip žmogaus rankų darbą. Žmogus turėtų suprasti, kad tai jis sukelia rizikas ir jis gali imtis veiksmų joms sumažinti ar išvengti.

Pasak šios teorijos autoriaus Ulricho Becko, o taip pat Anthony Giddenso, rizikos yra tapatinamos su naujos eros sukūrimu, t.y. moderniųjų laikų atsiradimu arba kitaip tariant rizika yra šiuolaikinio pasaulio pasekmė, todėl į ją reikėtų žvelgti kaip į žmogaus kūrinį. Rizikos atneštos modernizacijos yra visuotinos ir keliančios didesnę grėsmę nei anksčiau (Draper, 1993). Modernioje visuomenėje pagrindinėmis grėsmėmis yra laikomi vykstančių pokyčių šalutiniai poveikiai, kuriems pašalinti vis dar trūksta reikiamų žinių ir patirties (Taylor – Gooby, Zinn, 2006). Kitaip tariant žmogus

pats susikuria rizikas dėl, kurių vėliau baiminasi. Šioje teorijoje yra orientuojamasi į grėsmę kylančią iš paties žmogaus, kuria derėtų laikyti jo paties atsakomybe.

Rizikos visuomenėje kiekvienas asmeniškai stengiasi ieškoti informacijos susijusios su egzistuojančia rizika, kadangi nėra pasitikima ekspertais (Lupton, Tulloch, 2002). Vadinasi, šiuo atveju rizikos suvokimas yra perkeliamas į individualų rizikos suvokimo lygmenį.

Dar vienas reikšmingas aspektas siejamas su rizikos suvokimu yra **saugumo kultūra** *(angl. safety culture),* kuri nagrinėjama psichologiniu požiūriu. Saugumo kultūrą derėtų panagrinėti plačiau atsižvelgiant į tai, kad joje aiškiai atsispindi organizacijos rizikos suvokimas. Kuo stipresnė saugumo kultūra tuo geresnės apsisaugojimo ir pasirengimo priemonės vyrauja organizacijoje. Vadinasi, tokioje organizacijoje vyrauja galimų grėsmių supratimas. Rolfas Bye ir Gunnaras Lamvikas (2007) pastebi, jog Mary Douglas ir Aaronas Wildawsky‘s laikosi požiūrio, kad „individualus rizikos suvokimas atspindi socialinę situaciją“ (p. 133). Tai patvirtina, kad rizikos suvokimas atspindi organizacijos poziciją, požiūrį į saugumą. O saugumas organizacijoje yra pabrėžiamas, kai yra nustatomos rizikos ir tokiu būdu bandoma jas mažinti ar pašalinti (Hudson, 1999).

Saugumo kultūra yra aiškinama dviem aspektais. Viena vertus ji suprantama kaip įsitikinimai, požiūriai ar vertybės vyraujančios organizacijoje, kita vertus tai veiksmai, apimantys mokymus, pratybas, ekstremaliųjų situacijų planus (Reason, 1998; Borodzicz, 2005). Kadangi pastarasis aspektas yra apčiuopiamas ir aiškiau matomas, jis bus plačiau nagrinėjamas darbe (žr. 2 sk.).

Patrickas Hudsonas (1999) saugumo kultūrą aiškina kaip saugios aplinkos sukūrimą, kurios dėka bus išvengta neigiamų pasekmių, nes yra užtikrinamas aukšto lygmens saugumas, yra pateikiami būdai, padedantys ir nurodantys, kaip elgtis ekstremaliojoje situacijoje, o, be to, į organizacijos saugumo užtikrinimą yra įtraukiamas kiekvienas jos dalyvis.

Nagrinėjant pateiktus (Safety culture report, 1991) saugumo kultūros bruožus, atkreiptinas dėmesys į vieną iš jų. Vienas iš bruožų parodantis, kaip rizikos suvokimas yra siejamas su šiuo požiūriu yra *individualus saugumo įsisąmoninimas*. Tik aiškiai suvokus kas yra rizika ir ar ji tikrai egzistuoja galima kurti saugumo priemones. Taikant prevencines ar pasiruošimo priemones svarbu išaiškinti, kaip tos taikomos priemonės yra siejamos su nustatyta rizika. Tai yra svarbu dėl tos priežasties, kad individų rizikos suvokimas turėtų atitiki jiems taikomus reikalavimus saugumo srityje.

Organizacijos privalo pasirūpinti jos dalyvių rizikos suvokimu ir veiksmų, skirtų grėsmių sumažinimui inicijavimu. Jameso Reasono (1998) manymu, nepaisant vyraujančios silpnos saugumo kultūros, darbuotojai imsis saugumo priemonių, nes žinos apie gresiančius pavojus. Tačiau toks darbuotojų savisaugos elgesys, organizacijoje neskiriančioje dėmesio saugumo kultūros ugdymui, netruks ilgai. Autorius (Reason, 1998) pataria neignoruoti organizacijai kylančių grėsmių, kurios gali apsunkinti jos saugumo veiksmus. Tik žinančioje ir besiimančioje veiksmų, skirtų apsisaugoti nuo grėsmių, organizacijoje gali egzistuoti saugumo kultūra. Grėsmių mažinimo klausimu autoriui pritaria

Andrew Hopkinsas (2006), kuris pažymi, jog darbuotojai privalo būti skatinami suprasti, įsisąmoninti egzistuojančias rizikas su tikslu prisidėti prie saugios aplinkos kūrimo organizacijoje. Saugumo užtikrinimas yra ypač reikšmingas organizacijos veiksnys, kuriam nesant bus sutrikdytas organizacijos veikimas.

Kadangi saugumo kultūra atspindi rizikos suvokimą per organizacijos saugumo priemonių taikymą, t.y. pasirengimo veiksmus prieš ekstremaliąją situaciją, vadinasi, tiriant organizacijos pasiruošimą ekstremaliosioms situacijoms galima įžvelgti organizacijos rizikos suvokimą.

Iš **valdysenos teorijos** *(angl. governmentality)* pozicijos rizikos suvokimas yra nagrinėjamas kaip ekspertų ir valdžios institucijų kontrolės priemonė skirta palaikyti tvarką ir discipliną. Asmenys išeinantys iš už kontrolės ribų atsiduria rizikos zonoje (Lupton, 1999b). Tokiu būdu žmogus yra valdomas tų, kurie apibrėžia tai kas jam kelia grėsmę.

Roy Boyne (2003) pastebi, kad sprendimų priėmimas yra nulemtas ir priklauso nuo tų, kurie apibrėžia rizikos laipsnį. Autorius įvardina ekonomistus, matematikus, kognityvinius psichologus ir filosofus. Kitaip tariant tai žmonės, kuriuos galima įvardinti kaip ekspertus.

Visos apžvelgtos teorijos, paaiškinančios rizikos suvokimą yra nagrinėjamos skirtingais aspektais, todėl ir požiūris į riziką yra skirtingas.

Pastebimas skirtumas tarp valdysenos ir rizikos visuomenės teorijos yra tas, kad pastaroji atmeta ekspertų vaidmenį vertinant rizikas, kadangi individai stengiasi patys ieškotis informacijos susijusios su kylančiomis grėsmėmis ir vengia pasitikėti ekspertais. Priešingas į ekspertų požiūris yra išdėstomas valdysenos teorijoje, kuria remiantis būtent jie nustato, ką reikėtų suvokti kaip riziką. Skirtumas pastebimas tarp kultūrinės teorijos, kur rizikos suvokimas yra formuojamas remiantis visuomenės suvokimu, ir rizikos visuomenės, kuri pabrėžia individualumą aiškinantis suvokimą.

Šios teorijos patvirtina, kad rizikos suvokimas gali būti aiškinamas remiantis skirtingais požiūriais. Tačiau taip pat pastebėtina, kad šis suvokimas gali būti veikiamas įvairių faktorių.

Dauguma autorių (Paton ir kt., 2000; Tierney ir kt., 2001; Savadori ir kt., 2004; Renn, 2004) išskiria panašius arba vienodus veiksnius veikiančius rizikos suvokimą. B. Rohrmannas (2008) pateikia tokius veiksnius, turinčius įtakos rizikos suvokimui kaip grėsmės rūšys, asmeninė patirtis, įsitikinimai ir požiūriai bei įvairiapusė socialinė įtaka. Prie minėtų veiksnių yra priskiriamas rizikos suvokimas, sociokultūriniai ir sociodemografiniai faktoriai (Tierney ir kt., 2001; Lovekamp, Tate, 2008). D. Patonas ir kt. (2000) teigia, kad rizikos suvokimas priklauso nuo žmonių patirties, informacijos apie grėsmę interpretacijos ir informavimo šaltinių, kuriais jie pasitiki, turimų žinių bei klaidingų pažiūrų. Nagrinėjant rizikos suvokimą bandoma aiškintis, ar žinių laipsnis turi įtakos rizikos suvokimui. A. Wildavsky‘s ir Karlas Dake‘as (1990), bandydami išsiaiškinti, iki kokio laipsnio skirtingi žmonės vienodai jaudinasi dėl tų pačių grėsmių, kodėl vieni rizikas laiko didelėmis, kai tuo tarpu kiti tas pačias rizikas laiko mažomis, ištyrė žinių poveikį rizikos suvokimui. Tyrimo metu

paaiškėjo, kad labiau išsilavinę žmonės yra linkę įžvelgti mažesnę grėsmę, nei tie, kurie laiko save mažiau išsilavinusiais. Todėl buvo prieita prie išvados, kad rizikos suvokimas yra beveik nesusijęs su turimų savo žinių įvertinimu.

Atlikti tyrimai parodė, kad žmonių sugebėjimas suvokti riziką yra veikiamas daugybės veiksnių tiek vidinių, tiek išorinių. Kiekvieno individo ar grupės asmenų požiūris į rizikos suvokimą lemia jų elgesį veikti arba nesiimti jokių veiksmų ekstremaliųjų situacijų metu.

Žmonės skirtingai suvokia riziką dėl įvairių jau aptartų priežasčių. Tačiau yra išskiriamas ne tik pavienių individų rizikos suvokimas ir jų klasifikavimas pagal tam tikrus kriterijus, bet ir rizikos suvokimo skirtumai tarp dviejų grupių: visuomenės ir ekspertų. Tai būtų trečia išskirta rizikos suvokimo kategorija.

Ekspertų ir visuomenės nuomonių sutapimas tai retas reiškinys, kadangi dažniausiai šie požiūriai nesutampa. Aukštai įvardintas visuomenės rizikos laipsnis yra priešingai vertinamas ekspertų ir atvirkščiai. Ekspertų ir visuomenės nuomonių lyginimas rizikos suvokimo požiūriais parodo, kad abi grupės tas pačias rizikas vertina skirtingai. Tačiau į klausimą, kuri iš šių grupių riziką suvokia tokią, kokia ji yra iš tikrųjų yra sudėtinga. Taip pat yra išskiriami veiksniai, kurie parodo, kodėl tai kas yra nepriimtina ekspertams tampa įtikinama ir priimtina visuomenei ir atvirkščiai.

L. Sjobergas (1999) siekdamas išsiaiškinti, kodėl skiriasi ekspertų ir visuomenės rizikos suvokimo laipsnis nagrinėjo žinių ir informacijos asimetrijos veiksnius. Buvo bandoma suvokti, ar skirtumas tarp ekspertų ir visuomenės rizikos suvokimo yra paremtas informacijos stoka, t.y. visuomenė priešingai nei ekspertai neturi pakankamai informacijos tam tikrais nagrinėjamais klausimais. Atlikti tyrimai paneigė, kad visuomenės informacijos stoka yra pagrindinė priežastis, lemianti skirtingą rizikos suvokimą. Nepaisant to, kad tam tikrais klausimais visuomenė buvo informuota apie gresiančią riziką, vis dėlto kiekvienas individas elgėsi nepriklausomai nuo jam suteiktos informacijos. Nors žmonės gali suprasti jiems suteikiamą informaciją, vis dėlto tai nereiškia, kad jie galės ja tinkamai pasinaudoti (Paton, Johnston, 2001). Dažnai žmonės nesiima jokių veiksmų, nes yra įsitikinę, kad tai jų nepalies.

Na, o nagrinėdamas, rizikos suvokimo ir žinių santykį, autorius (Sjoberg, 1999) priėjo prie tokių pat išvadų kaip ir A. Wildavsky‘s ir K. Dake‘as (1990). Paaiškėjo, kad nors ir yra sąsaja tarp žinių ir rizikos suvokimo, vis dėlto ji yra nedidelė. Dėl šios priežasties rizikos suvokimas ne visada yra aiškinamas turimų žinių gausa. Taip pat pastebima, kad tam tikros srities ekspertai yra linkę įvardinti riziką mažesniu laipsniu nei visuomenė, todėl tai sukelia visuomenės susirūpinimą (Sjoberg, 1999, 2004; Renn, 2004).

Ekspertų ir visuomenės nuomonė rizikos suvokimo klausimais skiriasi dėl įvairių priežasčių. Visų pirma skirtumus lemia suvokiama kontrolė. Ekspertai dažnai nustato žemesnį rizikos laipsnį nei visuomenė, tikėtinai dėl to, kad save laiko labiau kvalifikuotais ir tinkamais rizikos įvertinimui, nes

gali kontroliuoti rizikas, be to ilgametė patirtis pripratino juos prie rizikų (Sjoberg, 1999; Fischhoff, 1995; Savadori ir kt., 2004). Tačiau ekspertai gali pervertinti savo turimas žinias ir patirtį, todėl tai gali tapti viena iš priežasčių, trukdančių jiems objektyviai įvardinti rizikos laipsnį.

Na, o visuomenės aukštą rizikos įvertinimą paaiškina tai, kad visuomenė yra linkusi priskirti aukštą rizikos laipsnį ir neigiamai vertinti tas rizikas, kurios yra „nežinomos, kelia didelę baimę“, yra „nekontroliuojamos“ ir „tikėtinai paveiks ateities kartas“ (Slovic, 1987, p. 285). Tikėtina, kad nepasitikėjimą ekspertais galima susieti su jau minėta rizikos visuomenės teorija, kurios požiūriu remiantis, visuomenė yra linkusi pati ieškotis informacijos, susijusios su kylančiomis grėsmėmis.

Vienas iš galimų būdų sugretinti visuomenės ir ekspertų rizikos suvokimą būtų visuomenės švietimas, tačiau P. Slovic‘iaus (1987) teigimu šis būdas nebūtų veiksmingas, kadangi žmonės aukštai įvertina tas rizikas, kurių atsiradimas yra mažai tikėtinas. Todėl prieštaravimai tarp ekspertų ir visuomenės išlieka.

Įtakos rizikos suvokimui turi ir tai, kokią reikšmę žodžiui *rizika* suteikia visuomenė ir ekspertai, pvz., visuomenė didesnį dėmesį atkreipia į tikimybę, tuo tarpu ekspertai susitelkia ties padariniais (Sjoberg, 1999; Slovic, 1987).

Viena vertus visuomenė yra priversta tapti priklausoma nuo ekspertų žinių, kita vertus ji suvokia, kad ekspertai ne tik gali suklysti apskaičiuodami ir nustatydami rizikas, bet taip pat ekspertų tarpusavio nuomonė dažnai išsiskiria. Tokie nenuoseklumai įvardijant rizikas skatina žmones mažiau pasikliauti ekspertų turimomis žiniomis (Tulloch, Lupton, 2002; Sjoberg, 1999; Savadori ir kt., 2004).

Kaip teigia Baruchas Fischhoffas (1995), ekspertai net ir turėdami informacijos apie rizikas yra linkę ją nuslėpti nuo visuomenės arba neužsimena apie jas, jei tos rizikos yra priimtinos visuomenėje. Nepaisant to, kad visuomenė skirtingai nuo ekspertų riziką suvokia remdamasi intuicija, emocijomis, savo patirtimi arba kasdienėmis žiniomis (Renn, 2004; Rimaitė, Rinkevičius, 2008), tačiau ekspertai nors rizikos suvokimą ir pagrindžia moksliškai, vis dėlto negalima teigti, kad tik ekspertų nuomonė yra patikima ir teisinga. Tokios pat pozicijos laikosi ir P. Slovic‘ius (1987), kuris nors ir pabrėžia, kad visuomenei arba kitaip tariant „ne specialistams“ trūksta žinių susijusių su grėsmėmis, vis dėlto jų rizikos suvokimas yra žymiai platesnis nei ekspertų, kurie dažnai apeina teisėtus interesus (p. 285). Tai yra paaiškinama tuo, kad ne tik visuomenei yra būdinga suklysti remiantis tokiais rizikos suvokimo kriterijais kaip klaidinga asmeninė patirtis, žiniasklaidos įtaka, bet ir ekspertams, kurie kaip ir visuomenė yra linkę pasikliauti savo intuicija, jei tuo metu neturi reikiamos informacijos.

Pastangos suvienodinti rizikos suvokimą tarp ekspertų ir visuomenės yra bevaisės. Kadangi kiekvienas įneša tam tikrą indėlį apibrėždamas gresiantį pavojų, todėl ignoruoti vienos ar kitos grupės rizikos suvokimo nėra teisinga, o be to, teigti, kad vien ekspertų nuomonė dėl rizikos suvokimo yra pagrįsta ir teisinga taip pat nereikėtų (Slovic, 1987). Analizuojant L. Sjobergo (1999) pateiktus veiksnius, skiriančius visuomenės ir ekspertų nuomonę, susidaro vaizdas, kad ekspertai paveikti įvairių

veiksnių gali suklysti įvardindami riziką. Todėl galima daryti prielaidą, kad ekspertai ne visada teisingai suvokia riziką.

Nepaisant to, kad tam tikros grupės žmonių bei įvairios mokslo sritys riziką apibrėžia skirtingai, vis dėlto svarbiausia, kad kiekviena organizacija suprastų kaip yra apibrėžiama ir suvokiama rizika toje organizacijoje, kad galėtų apsisaugoti nuo ekstremaliosios situacijos ir imtis apsisaugojimo veiksmų.

Remiantis įvairiais faktoriais ta pati rizika gali būti suvokiama skirtingai. Kadangi suvokimas priklauso nuo asmens nuomonės, įsitikinimų, pažiūrų, todėl tai yra vadinama subjektyviąja rizika. Interpretacijos susijusios su rizika priklauso nuo jai priskiriamos reikšmės, veikėjų, kurie ją interpretuoja ir pozicijų, iš kurių riziką yra nagrinėjama. Vertinant rizikos suvokimui turinčius įtakos veiksnius yra analizuojama patirtis, turimos žinios bei suteikiama informacija apie grėsmę. Tik esant sąmoningumui, kas yra rizika, įvertinus grėsmių pasireiškimo galimybę, galima imtis apsisaugojimo priemonių ir kurti stipresnę saugumo kultūrą. Nesuvokus rizikos nebus imamasi pasiruošimo veiksmų, kadangi nebus įžvelgiamas toks poreikis. Toks skirtingas rizikos suvokimo aiškinimas yra grindžiamas tuo, kad suvokimo aspektas yra nagrinėjamas iš skirtingų pozicijų.

2. RIZIKOS SUVOKIMAS IR JO ĮTAKA EKSTREMALIŲJŲ SITUACIJŲ VALDYMUI

2.1. Rizikos suvokimo svarba besiruošiant ekstremaliosioms situacijoms

Ekstremaliųjų situacijų metu rizikos suvokimas atlieka labai svarbų vaidmenį. Rizikos suvokimas sąlygoja individų elgesį imantis tam tikrų veiksmų, padėsiančių įveikti gresiančią ar susidariusią ekstremaliąją situaciją. Dėl šios priežasties netinkamas rizikos suvokimas, gali turėti neigiamą poveikį organizacijai. Perdėtas rizikos suvokimas sukelia paniką ir nereikalingus veiksmus, o nuvertinta rizika lemia veiksmų, reikalingų ekstremaliajai situacijai pašalinti arba sušvelninti, stoką. Tik įvertinta ir suvokta rizika gali padėti organizacijai tinkamai funkcionuoti ekstremaliųjų situacijų metu. Nepaisant to, kad organizacija gali nesugebėti užbėgti įvykiams už akių, vis dėlto adekvatus dėmesys pasiruošimui turi būti skiriamas.

Priklausomai nuo rizikos suvokimo kinta žmonių elgesys tiek prieš ar po ekstremaliosios situacijos arba jos metu. Suvokti gresiančią riziką ir žinoti kaip elgtis ekstremaliosios situacijos metu yra ypač svarbu, nes jos metu žmogus patiria stresą, tampa sudėtingiau priimti sprendimus (Paton, Flin, 1999; Rohrmann, 2008). Būtent todėl yra ypač svarbu skirti dėmesio į paruošiamajam etapui. Kadangi yra orientuojamasi į organizacijos gebėjimą veikti ekstremaliųjų situacijų metu, kuris apima sprendimų priėmimą, savo pareigų žinojimą, veiksmų, reikalingų išeiti iš susiklosčiusios situacijos ir kt., vadinasi, yra orientuojamasi į veiksmus, kurie yra išugdyti, išlavinti. O tai gali būti padaryta atliekant mokymus, rengiant įvairias pratybas. Vadinasi, organizacija siekianti tinkamai veikti ekstremaliosiose situacijose turi pasirūpinti, kad visi veiksmai būtų aptarti iki ekstremaliosios situacijos pradžios, t.y. pasiruošimo metu. Pasiruošimo procesas padeda pasirengti nenumatytiems, bet tikėtiniems įvykiams. Nepaisant to, kad neįmanoma numatyti visų įvykių ir nuo jų visiškai apsisaugoti, vis dėlto išankstinis pasiruošimas gali apsaugoti nuo nepageidautinų padarinių.

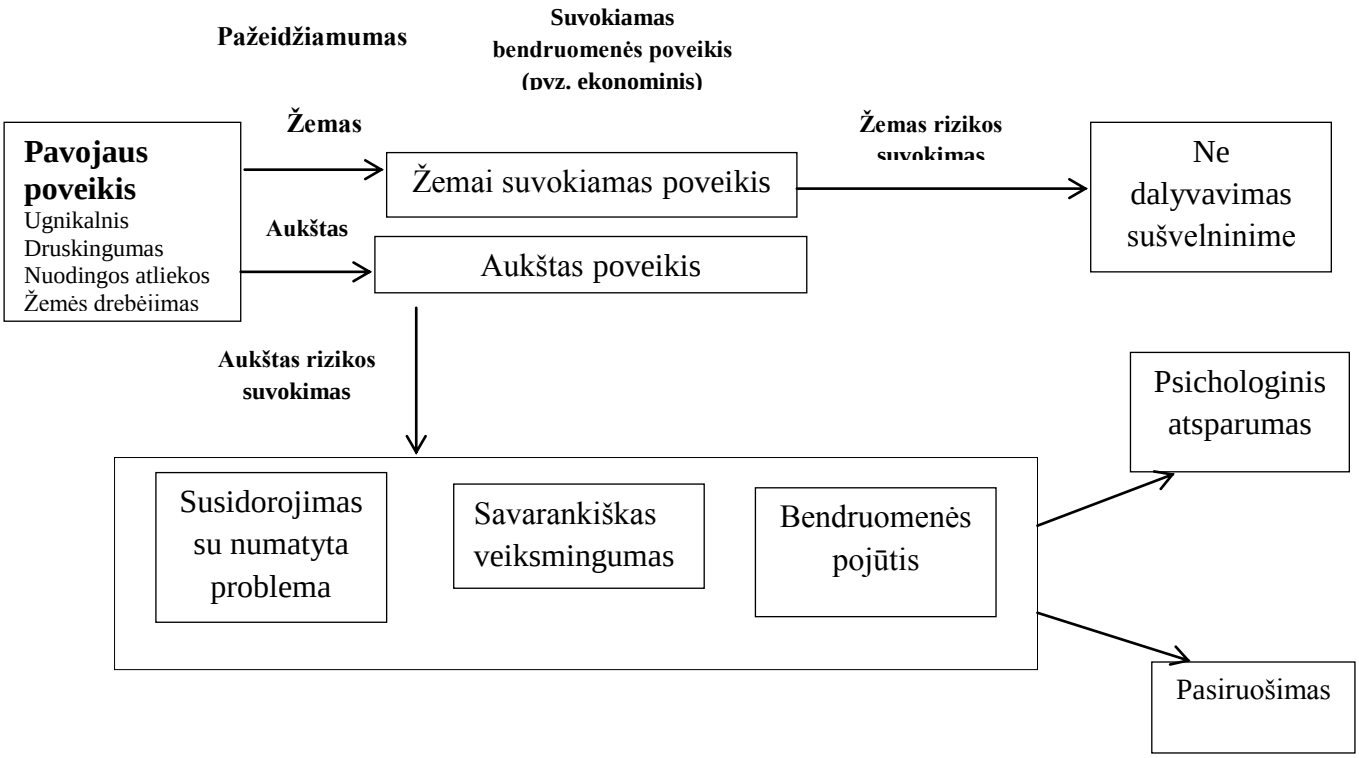
Rizikos suvokimas ir pasiruošimas ekstremaliosioms situacijoms yra glaudžiai susiję. Rizikos suvokimą veikia tam tikri faktoriai, kurie taip pat turi poveikio parengčiai. Tik suvokus galimų grėsmių riziką galima tinkamai joms pasiruošti.

Pasiruošimas ekstremaliosioms situacijoms turi užimti ypatingą vietą organizacijos veikloje, kadangi įvykusios situacijos gali sukelti grėsmę žmogaus gyvybei, socialinei aplinkai, jos susilpnina ne tik organizacijos finansinę struktūrą, bet ir jos įvaizdį (Mitroff ir kt., 1987). Organizacijos, kurioms yra didesnė rizika nei kitoms atsidurti ekstremaliojoje situacijoje, privalo itin kruopščiai rūpintis savo saugumu ir pakankamai dėmesio skirti pasiruošimui. Pasiruošimas apima planus ir veiksmus, užtikrinančius gebėjimą reaguoti į ekstremaliąsias situacijas ir sumažinti neigiamą padarinių poveikį

(Rutherford, 2008; Perry, Lindell, 2003). Davidas A. McEntire‘as ir Amy Myers (2004) pažymi, kad kalbant apie pasiruošimo procesą yra vadovaujamasi tuo, kad ekstremalusis įvykis gali įvykti. Vadinasi, yra daroma prielaida, kad yra tikimybė, jog nepageidaujamas įvykis ar situacija gali pasireikšti. Todėl siekiant nuo to apsisaugoti reikėtų susitelkti ties pasiruošimu. J. Rutherford (2008) į šį procesą žvelgia iš disciplinos ir būsenos pozicijų. Pasiruošimas yra laikomas disciplina, nes yra patikėta profesionalams ir valdžiai, kurie rūpinasi visuomenės saugumu ir užtikrina, kad kilus grėsmei jų saugumui ar sveikatai, jie bus apsaugoti. Žvelgiant į pasiruošimą kaip į būseną yra išryškinamas organizacijų tikslas užtikrinti, kad yra pasiruošta reaguoti ir susidoroti su iškylančiomis grėsmėmis. Panašų požiūrį pateikia R. W. Perry‘s, M. K. Lindellis (2003) ir M. K. Lindell ir kt. (2006), kurie į pasiruošimą žvelgdami kaip į būseną, teigia, kad „tai reagavimo į aplinkos grėsmes pasiruošimo būsena“ (p. 338), kurią sukuria veikla „iki įvykio“ *(angl. preimpact)*. Vadinasi, veikla iki įvykstant ekstremaliajai situacijai yra pagrindinė veikla, kuri atlieka svarbų vaidmenį jai įvykus ir po jos.

Organizacija siekdama apsisaugoti nuo ekstremaliųjų situacijų ir patirti kuo mažiau nuostolių turi būti tam tinkamai pasiruošusi. Ekstremalioji situacija savaime nėra kasdienis įvykis, todėl jos pasireiškimas kelia įtampą ir nerimą. Rizikos suvokimas šiuo aspektu atlieka svarbų vaidmenį, kadangi nuo rizikos suvokimo priklauso gresiančios situacijos įvertinimas, pasiruošimas jai ir reagavimas. Pasiruošimas ekstremaliajai situacijai yra svarbus, nes leidžia apsisaugoti nuo nepageidautinų padarinių arba bent minimaliai juos sumažinti, o taip pat apsibrėžti veiksmus po ekstremaliosios situacijos. Nesuvokus galimos rizikos nebus imamasi pasiruošimo veiksmų.

Apžvelgiant atsparumo pavojingiems padariniams modelį (3 pav.) pastebima, kad žmonės skirtingai suvokia savo pažeidžiamumą, t.y. vieni mano, kad yra labai pažeidžiami, kiti - kad jiems yra iškilusi mažesnė grėsmė. Šiame modelyje yra nagrinėjami trys tarpusavyje sąveikaujantys ir vienas nuo kito priklausantys elementai: pažeidžiamumas, rizikos suvokimas ir pasiruošimas. Analizuojant atvejį, kai bendruomenė ar organizacija suvokia save kaip labai pažeidžiamą, įžvelgiama, kad rizikos suvokimas bus aukštas, vadinasi, ji sieks apsisaugoti nuo nepageidaujamų padarinių ir, todėl tai paskatins ruošimąsi įvairioms ekstremaliosioms situacijoms, vadinasi, esant gerai parengčiai jos pažeidžiamumas mažės. O esant žemam pažeidžiamumui yra žemas ekstremaliosios situacijos poveikio suvokimas tam tikrai bendruomenei, todėl jų rizikos suvokimas yra žemas, vadinasi, nebus ruošiamasi arba mažai ruošiamasi ekstremaliosioms situacijoms, ko pasėkoje organizacija tampa labiau pažeidžiamesnė (Paton, Johnston, 2001; Mitroff, 1987). Taip pat pastebėtina, kad žmonės suvokiantys, kad kilusių grėsmių rezultatas bus nežymus ar nesijaučiantys turintys pakankamai kompetencijos veikti, pasižymės žemu pasirengimo laipsniu (Paton, 2003). Kadangi aukštos rizikos suvokimas sąlygoja paruošimą, todėl toks požiūris atskleidžia glaudų ryšį tarp rizikos suvokimo ir pasiruošimo ekstremaliosioms situacijoms.



3 pav. **Atsparumo pavojingiems padariniams modelis**

Šaltinis: Paton, Johnston, 2001, p. 271

Remiantis modeliu susidaro vaizdas, kad tie, kurie jaučiasi labiau pažeidžiamesni yra linkę sutelkti pastangas susidoroti su esama problema, bei ruoštis susidarysiančioms ekstremaliosioms situacijoms. Svarbu tai, kad juos veikia bendruomeniškumas. Manytina, kad šis modelis taip pat gali būti pritaikomas organizacijose su tikslu įvertinti, kaip pasiruošimas yra veikiamas rizikos suvokimo, ar organizacija laiko save pažeidžiama, kaip suvokia ekstremaliosios situacijos padarinių poveikį savo veiklai. Šis modelis patvirtina, kad priklausomai nuo rizikos suvokimo yra organizuojama arba ignoruojamas pasiruošimas ekstremaliosioms situacijoms.

Kadangi rizikos suvokimas yra susijęs su pasiruošimu ekstremaliosioms situacijoms, todėl vertėtų susirūpinti rizikos suvokimo pokyčiais, atsirandančiais po įvykio. Po susidūrimo su ekstremaliuoju įvykiu sustiprėja susirūpinimas gresiančia problema, todėl tai teigiamai veikia pasiruošimą. Tačiau grėsmei praėjus susirūpinimas sumažėja, kas lemia mažesnį pasiruošimą ekstremaliosioms situacijoms (Tierney ir kt., 2001). Pervertindama savo apsisaugojimo jėgas ir nesiimdama tinkamų savisaugos priemonių organizacija gali pati sau pakenkti. Anot Iano I. Mitroffo (2006), organizacija yra pasmerkta neatsigavimui po ekstremaliosios situacijos, jei ji (p. 71):

- sąmoningai ignoruoja pavojaus signalus,
- nesiima jokių prevencijos ir pasiruošimo veiksmų,
- nesiėmė jokių veiksmų sustabdyti padarinių išplitimą.

Šie veiksmai patvirtina, kad svarbu yra sutelkti dėmesį į pasiruošimą, kurio vaidmuo yra ypač svarbus organizacijai. Priešingu atveju tokiai organizacijai bus sudėtinga atsigauti po ekstremaliosios situacijos.

Nuo organizacijos veiksmų priklauso, kaip vystysis tolesnė jos veikla, todėl siekiant išvengti neigiamų padarinių, svarbu imtis prevencinių priemonių. Kadangi pasiruošimo ekstremaliosioms situacijoms tikslas yra „padidinti socialinių vienetų *(angl. social unit)* gebėjimą reaguoti ekstremaliosios situacijos atveju“ (Tierney ir kt., 2001, p. 27), todėl galima teigti, kad pasiruošimo proceso dėka yra prisidedama prie veiklos ekstremaliosios situacijos metu, o taip pat šis procesas palengvina tolimesnių veiksmų kryptį. Kuo kruopštesnis yra pasiruošimas, tuo paprasčiau galima susidoroti su esama padėtimi po ir jos metu.

Organizacija turi gebėti reaguoti į įvykstančias ekstremaliąsias situacijas. Visos ekstremaliųjų situacijų valdymo proceso fazės yra svarbios ir turi būti įgyvendinamos. Tačiau viena esminių fazių, turinti reikšmės tolimesnėms fazėms ir veiksmams yra pasiruošimas. Esant geram pasiruošimui, galima tinkamai ir greitai reaguoti į įvykį, o numačius galimas grėsmes imtis reikiamų atsigavimo priemonių.

Pasiruošimas padeda imtis „prevencijos priemonių, sušvelninti gresiančią riziką, reaguoti ir atsigauti“ (Radvanovsky, 2006, p. 76). Todėl nepaisant to, kad ekstremaliųjų situacijų valdymas yra ciklišKas procesas, vis dėlto galima tvirtinti, kad pasiruošimas sudaro kitų veiksmų ar fazių veikimo pamatą bei užima reikšmingą vietą šiame procese. Pasirengimo svarbą pažymi ir tai, kad nesant pasiruošimui bei planams neįmanoma sulaukti pageidautino atsako šalinant ar sušvelninant ekstremaliųjų situacijų padarinius, o taip pat greitai grįžti į pradinę būseną (Jackson ir kt., 2011; Mitroff ir kt., 2006). Tik tinkamai suvokus esamą pažeidžiamumą ir gresiančią riziką galima tinkamai paveikti pasiruošimo procesą.

Požiūrį į rizikos suvokimą formuoja ir įtakos ekstremaliųjų situacijų pasiruošimui turi ne tik pažeidžiamumo suvokimas, bet ir iškreiptas optimizmas *(angl. optimistic bias)*. Žmonės lydimi iškreipto optimizmo lygindami save su kitais žmonėmis teigia, kad yra geriau pasiruošę nei pastarieji, nors ne visais atvejais tai pasitvirtina (Paton, Johnston, 2001). Tokiu atveju yra tikima, kad nelaimė gali paliesti kitus, bet ne konkrečiai tą asmenį. Anot Neilo D. Weinsteino (1989), iškreiptas optimizmas yra priežastis to, kad nėra apsisaugojama nuo riziką skatinančio elgesio. Šis suvokimas pasireiškia tada, kai galimų grėsmių atsiradimo tikimybė yra maža ir manoma, kad jos gali būti suvaldomos ir, kai turima mažai patirties su grėsmėmis. Nesant ankstyvų pažeidžiamumo ženklų yra tikima, kad ateityje bus išvengta grėsmių. Toks iškreiptas optimizmas turi daugiau neigiamo poveikio nei teigiamo, kadangi gali nulemti netinkamą elgesį prieš ekstremaliąją situaciją. Pastarasis požiūris patvirtina, kad vyraujantis rizikos suvokimas trukdo įvertinti rizikos stiprumą ir svarumą. Todėl

darytinos prielaidos, kad minėtasis iškreiptas rizikos suvokimas reiškia, kad pasiruošimas ekstremaliųjų situacijų valdymui taip pat bus iškreiptas ir nepakankamas.

Nagrinėjant rizikos suvokimą buvo aptarti įvairūs ją sąlygojantys veiksniai, vienas iš jų yra informacijos suteikimas, kuris manytina, taip pat gali turėti poveikį parengčiai. Tačiau D. Patonas (2003) teigia, kad aprūpinimo informacija negalima įvardinti kaip esminio faktoriaus, turinčio poveikį pasiruošimui ekstremaliosioms situacijoms. Ignoruojant informaciją susirūpinimas grėsmėmis sumažės, todėl tai nepaveiks teigiamai pasiruošimo proceso. Collinas Powellas (2007) paaiškina, kad ignoruojama ir atmetama informacija yra, jei ji nesutampa su esamomis asmens nuostatomis ar požiūriais. Na, o išsamios informacijos suteikimas nereiškia, kad visi reaguos vienodai ir imsis saugumo priemonių. Nes, pasak K. J. Tierney ir kt. (2001), svarbu yra suteiktos informacijos įvertinimas, naujos paieška, kitaip tariant svarbu įvertinti, kaip žmonės panaudoja jiems suteiktą informaciją ir kokią prasmę jai suteikia. Kadangi net priėmus ir supratus pateikiamą informaciją, pasiruošimo veiksmai gali būti atidėti arba išvis jų nebus imtasi ateityje. Ši situacija atskleidžia, kad ignoruojant suteikiamą informaciją arba pakankamai jos neįvertinus yra neaiškiai formuojamas rizikos suvokimas.

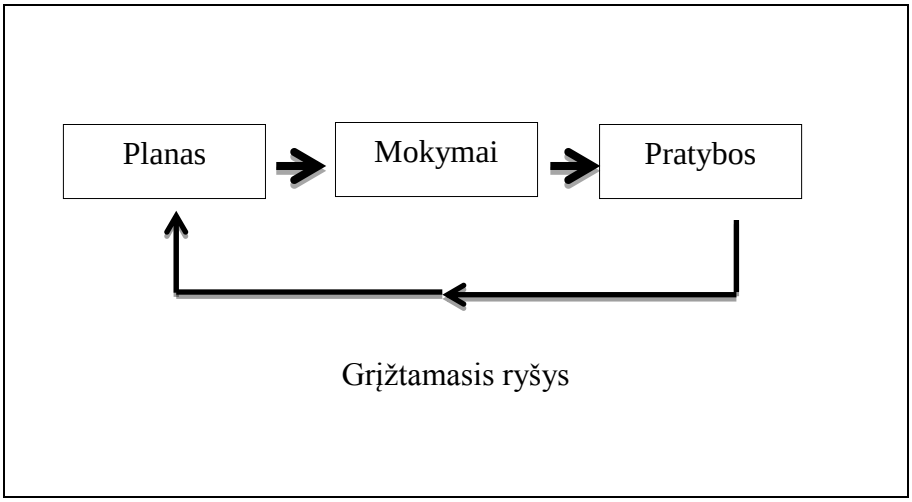
Priklausomai nuo rizikos suvokimo yra formuojamas elgesys ir požiūris kaip reikėtų veikti ekstremaliosios situacijos metu ir prieš ją. Rizikos suvokimas, kuris turi įtakos pasiruošimui, yra sąlygotas pažeidžiamumo ir iškreipto optimizmo veiksnių. Suvokimas esant pažeidžiamam skatina imtis pasiruošimo priemonių galimai grėsmei, kadangi rizika yra laikoma aukšto laipsnio bei turinti poveikio objektui ir atvirkščiai. O iškreiptas optimizmas neigiamai veikia pasiruošimą, kadangi skatina teigiamai galvoti apie apsisaugojimo priemones, kurių realybėje gali nebūti. Informacija, kuri suteikia galimybę apsvarstyti savo elgesį ir veiksmų planą, nėra tinkamas kriterijus nustatantis ryšį tarp rizikos suvokimo ir pasiruošimo.

2.2. Pasiruošimo veikti ekstremaliosiose situacijose priemonės

Pasiruošimas ekstremaliosioms situacijoms nėra laikomas svarbiu organizacijos uždaviniu, kadangi nėra įžvelgiama rizikų galinčių paveikti jos veiklą. Vyraujant tokiam suvokimui organizacijos neskiria dėmesio planų, padėsiančių susidoroti su įvykusia situacija kūrimui. Tokia organizacijos pozicija gali būti pražūtinga jos tolimesniam veiklos plėtojimui.

Nagrinėjant mokslininkų darbus pasiruošimo srityje, pastebimi įvairūs jos elementai. Yra mokslininkų (Perry, 2004; Rutherford, 2008), kurie savo darbuose susitelkia ties keliais pasiruošimo žingsniais, kaip antai, planų kūrimas, mokymai ir pratybos, kiti (Radvanovsky, 2006) pateikia jų daugiau. Todėl pasiruošimo etape yra įvardijami tokie veiksmai kaip mokymai, politikos, planų ir procedūrų sudarymas, darbuotojų kvalifikacijos kėlimas, pratybos, apsirūpinimas reikalinga įranga.

Kiekviena organizacija gali būti paveikta ekstremaliosios situacijos ir tai gali sutrikdyti jos veiklą. Siekdamos sėkmingai ją atnaujinti, jos turėtų susitelkti į pasiruošimo procesą ir įvertinti priemones, kurios padėtų suformuoti rizikos suvokimą. Atsižvelgiant į tai, darbe nuspręsta analizuoti tęstinės veiklos planavimo tris svarbius žingsnius, kurie yra laikomi pasiruošimo ekstremaliosioms situacijoms dalimi, t.y. planavimą, mokymą ir pratybas (4 pav.).



4 pav. **Pasiruošimo ekstremaliosioms situacijoms procesas**

Šie veiksmai yra glaudžiai tarpusavyje susiję, nes tik nusistačius aiškius veiksmus, kokių reikėtų imtis įvykus ekstremaliajai situacijai galima vykdyti mokymus ir pratybas. Mokymų ir pratybų metu gali išryškėti plano trūkumai, tačiau į tai reikėtų žvelgti teigiamai, kadangi tai suteikia galimybę patobulinti sukurtą planą bei pašalinti iškilusius trūkumus. Į šiuos tris etapus reikėtų žvelgti kaip į visumą, bet ne atskirai. Nesant bent vienam iš šių elementų sudėtinga būtų sudaryti veiksmingą planą, skirtą išvengti neigiamų padarinių. Organizacijos požiūris į plano, mokymų bei pratybų poreikį gali atskleisti joje vyraujanti rizikos suvokimą.

2.2.1. Tęstinės veiklos plano rengimas

Įvykusi ekstremalioji situacija gali sukelti neigiamus padarinius ne tik organizacijai, bet ir ją supančiai aplinkai. Dėl šios priežasties, susidarius ekstremaliajai situacijai svarbu būti pasiruošusiems veikti. Veikimas gali būti tik tada, kai yra žinoma kokių priemonių reikia imtis siekiant susidoroti su esama padėtimi, t.y. kai yra planas. Todėl vienas svarbesnių žingsnių, kurį galima laikyti pasiruošimo pamatu, yra planavimas.

K. J. Tierney ir kt. (2001) pabrėžia, kad yra išskiriamos skirtingos ekstremaliųjų situacijų pasiruošimo procesui veiklos priklausomai nuo organizacijos pobūdžio, t.y. privatus ar viešas sektorius, bendruomenės ar namų ūkiai. Nepaisant organizacijos pobūdžio kiekviena jų turi turėti planus, reikalingus veikti ekstremaliųjų situacijų metu ir po jų.

Nagrinėjant pasiruošimo ekstremaliosioms situacijoms plano sudarymą, pastebima, kad daugiausia orientuojamasi yra į viešojo sektoriaus galimybes susidoroti su įvykusia situacija (Tierney ir kt., 2001). Tai reglamentuoja teisės aktai, kuriamos taisyklės, planai ir kt. Tuo tarpu privačiam sektoriui yra paliekama pasirinkimo laisvė pačiam apsispręsti dėl organizacijos saugumo užtikrinimo. Denniso S. Mileti (1999) kaip ir K. J. Tierney ir kt. (2001) teigimu, daugiausia pasirengimas yra pabrėžiamas viešajame sektoriuje negu kitokio pobūdžio organizacijose. Autorių manymu, privataus sektoriaus organizacijos nėra linkusios imtis pasiruošimo veiksmų, kadangi jos nėra įpareigotos to daryti ir gali nuspręsti to imtis savo nuožiūrą.

Manytina, kad kiekviena organizacija įskaitant privatų sektorių privalėtų turėti planus, padėsiančius jai ne tik pasiruošti, bet ir užtikrinti savo veiklos plėtrą po ekstremaliosios situacijos. Tai yra svarbu, nes ji turi sugebėti ne tik atkurti turėtus duomenis, bet ir išsaugoti savo įvaizdį. Kaip teigia Ali H. Al-Badi ir kt. (2008) - „veiksmingas ekstremaliosios situacijos planavimas nėra fakultatyvus, jis yra lemiamas veiksnys organizacijos sėkmei“ (p. 114). Būtent dėl šios priežasties organizacija siekianti visokeriopos sėkmės turėtų susitelkti į plano rengimą. Plano turėjimas ir sugebėjimas juo pasinaudoti priklauso nuo to, kaip organizacija suvokia jai kylančias rizikas ir parodo organizacijos pasiruošimą nenumatytoms, bet galimoms grėsmėms. Tokio plano svarba yra ypač pabrėžiama informacinių technologijų srityje.

Paprastai į planavimą yra žvelgiama kaip į veiksmą, kuris susijęs tiek su pasiruošimu, tiek su reagavimu. Kaip teigia R. W. Perry, M. K. Lindell (2003), planavimas yra pasiruošimo dalis, kurio tikslas yra „grėsmių įvertinimas ir rizikos sumažinimas“ (p. 339). Kadangi grėsmių įvertinimas remiasi ne tik jau įvykusiomis, bet ir dar įvyksiančiomis grėsmėmis, todėl gali būti pritaikomas ir tose organizacijose, kurios dar nebuvo paveiktos grėsmių. I. I. Mitroff (1987) ir R. W. Perry (2004) planavimą sieja su reagavimu, kadangi planavimas moko organizaciją kaip susidoroti su iškilusiomis problemomis ir palengvina jos grįžimą į įprastinę būseną. Viena vertus planavimas yra artimesnis parengčiai, nes sudaro jos pagrindą. Kita vertus negalima paneigti sąsajos tarp planavimo ir reagavimo, kadangi planavimo metu yra apsibrėžiama, kaip bus reaguojama į ekstremaliąją situaciją.

Planavimas tai veiksmai arba pasiruošimas, apimantis prioritetų bei funkcijų nustatymą, mokymų vykdymą, išteklių įsigijimą, žmogiškųjų ir kitų išteklių bei įrangos naudojimą, kurie atliekami iki įvykstant tam tikrai situacijai. Tai veiksmai, kurie yra atliekami esant įprastomis sąlygomis ir jų paskirtis yra pagelbėti ekstremaliųjų situacijų metu, užtikrinant tinkamą komunikavimą, įrangos ir kitų sistemų veikimą (Perry, 2004; Radvanovsky, 2006). Vadinasi,

planavimas turi vykti nuolat, kažką keičiant ar pildant, tai turi būti tęstinis procesas, nuo kurio priklauso organizacijos pasiruošimas ir elgesys įvykus nelaimei.

Ne tik individų elgesį ir veiksmus ekstremaliosios situacijos metu, prieš ir po jos sąlygoja tai, kaip jie suvokia riziką, bet tai galioja ir organizacijoms. Organizacijai yra labai svarbu suvokti galimų grėsmių riziką, kadangi tai turės įtakos pasiruošimo plano sudarymui. Tinkamą planavimą organizacija gali užtikrinti tik tada, jei yra tinkamai pasiruošusi, o šį pasiruošimą gali sąlygoti tęstinės veiklos plano *(angl. business continuity plan)* sukūrimas. Šio plano esmę sudaro galimų rizikų įvertinimas ir valdymas, jų sukeltų padarinių poveikis ir apskaičiavimas, ką reikia saugoti (Al-Badi ir kt., 2008).

„Tęstinės veiklos planas tai planas ar procedūra, kuri užtikrina savalaikį ir organizuotą tęstinumą ar greitą veiklos atkūrimą po ekstremaliosios situacijos“ (Kildow, 2011, p.5). Anot autorių (Cerullo, Cerullo, 2004; Kildow, 2011), nesant šiam planui tikėtina, kad atsigavimo po ekstremaliosios situacijos procesas užtruks. Būtent todėl siekiant to išvengti svarbu turėti tęstinės veiklos planą.

Tęstinės veiklos plano svarba gali būti lemiama organizacijai, kadangi jo neturint galima neatsigauti po ekstremalaus įvykio, nes bus prarasta informacija, sugadinta įranga. Šio plano poreikį patvirtina surinkta autoriaus (Al-Badi ir kt., 2008) informacija, jog 90 procentų verslo įmonių, kurios praranda duomenis ekstremaliosios situacijos metu nutraukia savo veiklą, kita dalis nesugeba atsigauti po įvykio, grįžti į įprastinę būseną, todėl taip pat yra priverstos nutraukti savo veiklą. Neturėdama plano organizacija nesugebės greitai reaguoti į susiklosčiusią padėtį, todėl ilgų metų darbo pastangos gali būti sunaikintos.

Pasak Virginia Cerullo ir Michaelo J. Cerullo (2004), tęstinės veiklos planavimo procesas susideda iš trijų pagrindinių elementų:

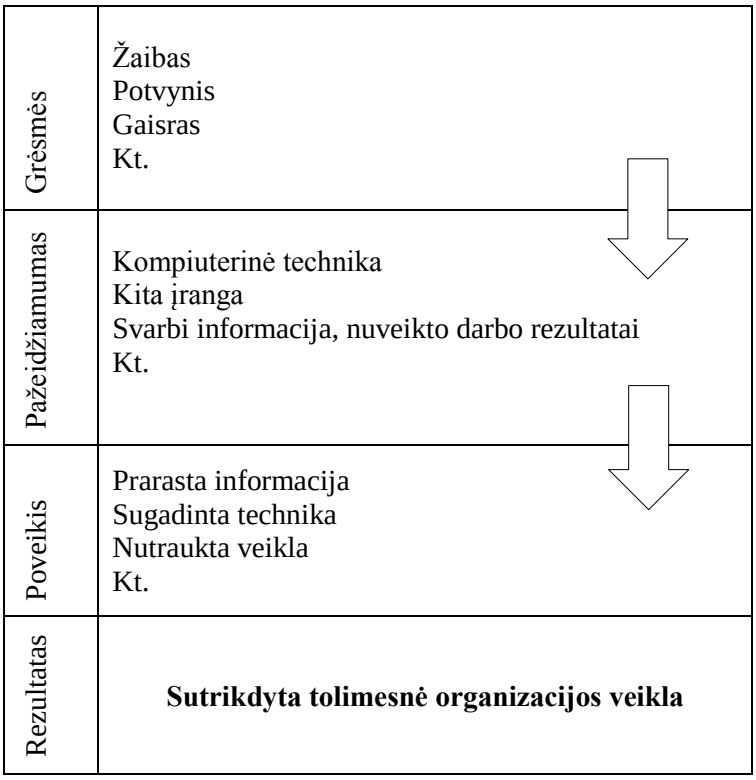
- Pagrindinių rizikų identifikavimo;
- Plano, padėsiančio sušvelninti išskirtų rizikų poveikį, sukūrimo;
- Darbuotojų apmokymo ir plano veiksmingumo patikrinimo.

Siekiant pereiti prie plano kūrimo proceso ir pradėti analizuoti šiuos tris žingsnius svarbu prisiminti rizikos elementus, be kurių tolimesnė analizė bus negalima.

Taigi rizika susideda iš **grėsmės**, **tikimybės**, kad grėsmė pasireikš, organizacijos **pažeidžiamumo** šiai grėsmei ir galimo jos **poveikio**. Pažeidžiamumo įvertinimas nustato, kaip labai pažeidžiama, jautri ir pasiduodanti tam tikroms grėsmėms yra organizacija bei kokia yra tikimybė, kad ta grėsmė pasireikš. Kitaip tariant pažeidžiamumas parodo organizacijos silpnąsias vietas. Įvertintas pažeidžiamumas ir tikimybė sudaro poveikio įvertinimo pagrindą. Poveikio įvertinimas analizuoja kaip stipriai grėsmės atsiradimas paveiks organizaciją (Snedaker, 2007).

Siekiant patvirtinti tęstinio veiklos planavimo poreikį buvo sudarytas galimų grėsmių scenarijus (5 pav.). Kadangi tyrimui atlikti ir nagrinėti buvo pasirinkta informacinių technologijų organizacija, todėl šis scenarijus taip pat parengtas atsižvelgiant į IT organizacijos veiklos pobūdį. Šios

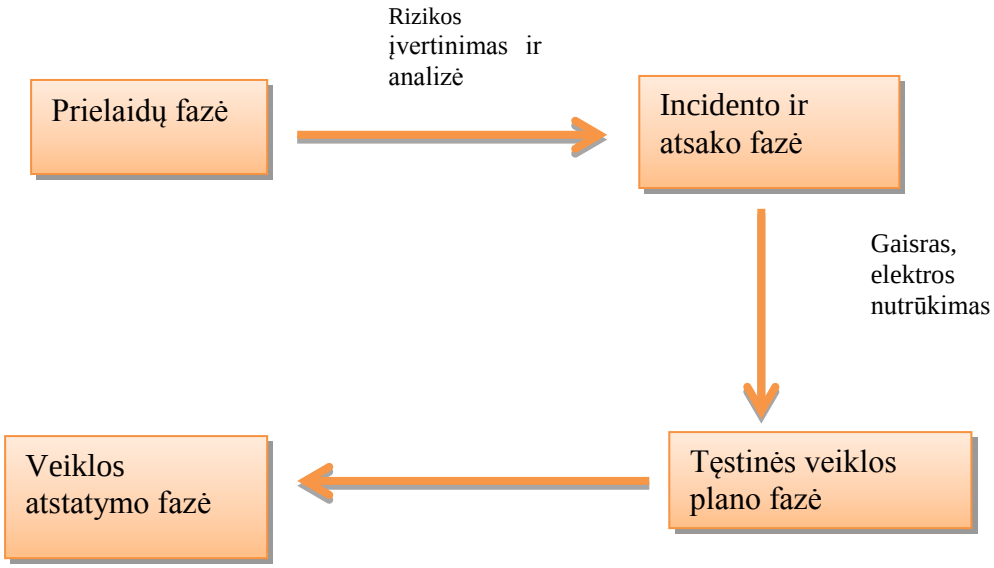
organizacijos pasirinkimą lėmė tai, kad dėl savo veiklos pobūdžio organizacija susiduria su įvairiomis grėsmėmis ir todėl, manytina, ji yra pažeidžiama. O naujų grėsmių atsiradimas skatina organizaciją saugotis tiek nuo vidinių, tiek nuo išorinių rizikų, dėl šios priežasties ji turi būti gerai pasiruošusi įvairiems netikėtumams. Kadangi tęstinės veiklos planavimas prasidėjo būtent nuo siekio apsaugoti informacines sistemas, todėl šis planas yra tinkamas įvertinti kokių veiksmų organizacija imtųsi siekdama apsisaugoti savo veiklą nuo ekstremaliųjų situacijų. Bandant išsiaiškinti, kodėl organizacijai yra svarbu užtikrinti savo veiklos tęstinumą buvo analizuojamas galimų grėsmių scenarijus.



5 pav. **IT galimų grėsmių scenarijus**

Bandant patvirtinti pasiruošimo ekstremaliosioms situacijoms plano poreikį, buvo išnagrinėtos galimos grėsmės galinčios turėti poveikio organizacijos veiklai dėl jos pažeidžiamų sričių. Pvz., pasireiškus žaibui gali būti sutrikdytas elektros tiekimas, tai nutrauks kompiuterių veiklą, todėl tuo metu gali būti prarasta svarbi informacija. Visa grandinė šių veiksmų gali apriboti organizacijos veiklą. Todėl yra reikalingas planas, apibrėžiantis organizacijos veiksmus.

Siekiant kuo skubiau grįžti į įprastinės veiklos vykdymą svarbu suvaldyti gresiančias rizikas. Tai galima padaryti pereinant per keturias rizikos įgyvendinimo fazes (6 pav.).



6 pav. **Rizikos įgyvendinimo fazės**

Pirmojoje prielaidų fazėje yra atliekamas rizikos įvertinimas ir analizė, kurių dėka yra identifikuojamos problemos ir veiksmai, kurių reikėtų imtis įvykus ekstremaliajai situacijai. Atliekant rizikos analizę yra nagrinėjama kiekybinė rizika vertinant jos pasireiškimo tikimybę bei kokybinė rizika analizuojant grėsmes ir pažeidžiamumus. Sekančioje incidento ir atsako fazėje organizacija turi įvertinti įvairius galimus incidentus, kurie gali paveikti jos veiklą. Atlikta poveikio analizė padeda organizacijai suvokti galimą praradimą, jeigu įvyktų ekstremalioji situacija. Taigi nustačius rizikas, galinčias turėti neigiamą poveikį organizacijos veiklai yra įvertinamas jų galimas poveikis bei rizikos atsiradimo tikimybė. Rizikos ir poveikio analizė gali pagelbėti įvertinant į kokius įvykius reikėtų atkreipti daugiausia dėmesio kuriant tęstinės veiklos planą (Blades, 2001; Savage, 2002; Cerullo, Cerullo, 2004). Įvairios galimos grėsmės turi atsispindėti organizacijos plane. Tęstinės veiklos plano fazė leidžia organizacijai išlikti ir toliau tęsti savo veiklą po ekstremaliosios situacijos, įgalina toliau teikti jai būdingas paslaugas. Tačiau pažymėtina tai, kad ši fazė yra tik kaip „pirmoji pagalba“ po incidento. O norint, kad organizacija visiškai atsigautų ji turėtų pereiti į paskutiniąją veiklos atstatymo fazę, po kurios galės vykdyti jai įprastas funkcijas (Blades, 2001).

Pasiruošimo metu yra pabrėžiama bendradarbiavimo (Tierney ir kt., 2001; McEntire ir Myers, 2004; Blyth, 2008) tarp įvairių organizacijų bei ekspertų ir „ne specialistų“ svarba. K. J. Tierney ir kt. (2001) teigimu, yra klaidinga manyti, kad ekstremaliųjų situacijų valdymas ir sprendimų priėmimas jų metu gali būti valdomi vieno subjekto. Autoriai pabrėžia, kad augant ekstremaliųjų situacijų mastams, jų valdyme dalyvaujančių subjektų skaičius taip pat turi išaugti. Organizacijos negali veikti vienos, jos pasiruošimo planus turėtų rengti atsižvelgiant į kitų organizacijų dalyvavimą. Rengiant minėtus planus patartina, kad dalyvautų kuo daugiau darbuotojų atsižvelgiant į grupių ir individų rizikos suvokimą, į

tai, kas yra laikoma grėsme. Kadangi pasiruošimo lygis priklauso nuo to, kaip bus priimta informacija apie pavojų, ar ji bus laikoma patikima, ar gresiantis įvykis tiesiogiai lies individus.

Rengti nepaprastųjų situacijų planus yra labiau orientuotos ir suinteresuotos tos organizacijos, kurios atlieka pavojingas funkcijas, o tos, kurios įgyvendina mažiau pavojingas funkcijas sunkiau įsitraukia į planų rengimą (Tierney ir kt., 2001). Tačiau yra tokių organizacijų, kurių planų rengimą reglamentuoja teisės aktai, todėl jos yra įpareigotos įsitraukti į pasiruošimo ekstremaliosioms situacijoms procesą.

Teisės aktų nustatyta tvarka tam tikros institucijos yra įpareigotos parengti ekstremaliųjų situacijų valdymo planus. Ypač viešojo sektoriaus ar organizacijos vykdančios pavojingą veiklą. Vis dėlto ne visos organizacijos skiria pakankamai dėmesio plano rengimui, ypač tos, kurios turi pasirinkimo laivę. Šiai kategorijai gali būti priskiriama tyrinėjama IT organizacija, kuri apie tokio plano būtinybę nusprendžia įvertinusi rizikas.

Priežastys dėl kurių organizacijos vengia rengti pasiruošimo planus yra tos, kad jie nėra laikomi prioritetine sritimi (Tierney ir kt., 2001; Lindell ir kt., 2006; Vancoppenolle, 2007):

- *Grėsmių nuvertinimas* yra viena pagrindinių priežasčių, kodėl organizacijos nėra linkusios imtis paruošiamųjų darbų ar kurti apsisaugojimo nuo ekstremaliųjų situacijų planus. Taip yra, todėl, nes egzistuoja suvokimas, kad grėsmės gali paliesti kitus, o jų atsiradimo tikimybė yra tokia menka, kad planų kūrimo procesas nepasiteisins ir neapsimokės.
- *Per dideli kaštai (išteklių nepakankamumas).* Planavimas tai sudėtingas procesas, kuris reikalauja didelių finansinių ir žmogiškųjų išteklių. Kai organizacijos biudžetas yra ribotas, o prioritetine sritimi nėra laikomas apsisaugojimas nuo galimų grėsmių, tada pasirengimo planai tampa antraeiliais. Organizacija gali nesuvokti tokio plano svarbos tuo atveju, jei ji nesuvokia jai gresiančios rizikos.
- *Nenoras pripažinti savo pažeidžiamumo.* Esant planui, skirtam apsisaugoti nuo gresiančių rizikų, organizacijai gali atrodyti, kad tokiu būdu ji parodo savo pažeidžiamumą.
- *Neįtraukiama į organizacijos tikslus.* Didžioji dalis organizacijų, pasiruošimo planus laiko šalutiniais dalykais, kurie neįeina į organizacijos tikslus. Dažnai dėl to, kad gresianti rizika yra nuvertinama, nes ekstremaliosios situacijos yra laikomos mažai tikėtinomis.
- *Per sudėtingas įgyvendinimas.* Siekiant parengti kokybiškus ekstremaliųjų situacijų pasiruošimo planus reikėtų atlikti detalią grėsmių analizę, kurią sudėtinga įgyvendinti, o tikslai yra neaiškiai išreikšti.

Jeigu organizacija aiškiai suvokia jai gresiančias rizikas, tokiu atveju aukščiau paminėtos priežastys neturėtų sukelti sunkumų rengiant pasiruošimo ekstremaliosioms situacijoms planus.

Planas apibrėžia kiekvieną veiksmą, kurio turi būti imtasi. Rengiant planus reikėtų nepamiršti, kad jie turi būti ne bendro pobūdžio ar preliminarūs, bet konkretūs, aiškūs, atspindintys tikrąją situaciją bei pritaikyti konkrečiai organizacijai, priklausomai nuo jai kylančių grėsmių (Tierney ir kt., 2001; Perry, 2004; Blyth, 2008). Plano rengimo metu svarbu atsižvelgti ir į tai, kad grėsmės su laiku keičiasi, todėl plane nereikėtų vadovautis praeities praktika, o tobulinti ir ieškoti naujų būdų, padėsiančių susidoroti su naujomis grėsmėmis (Quarantelli, 1993).

Nepaisant to, kad ekstremalioji situacija tai netikėtas įvykis dėl kurio ne visada galime būti tikri ir todėl planas negali numatyti visų rizikų ir nuo jų apsaugoti (Perry, 2004), vis dėlto jo sudarymas užtikrina, kad organizacija bus pasirengusi susidoroti su grėsmėmis. Pasiruošimas ekstremaliosioms situacijoms turi užimti itin svarbią vietą organizacijos veikloje. Organizacija privalo turėti planus, skirtus ekstremaliajai situacijai valdyti. Planai, padėsiantys veikti ekstremaliosios situacijos metu privalo būti itin kruopščiai rengiami. Juose numatant galimas rizikas atsispindi kaip ekstremaliosios situacijos atveju bus naudojama turima įranga, kas ir kokius veiksmus atliks, kokios bus taikomos prevencijos priemonės.

Toks planavimo procesas turi pasižymėti lankstumu tam, kad galėtų prisitaikyti prie besikeičiančių ekstremaliųjų situacijų (Perry, Lindell, 2003). Tačiau svarbu ir tai, kad „geras planavimas nebūtinai tampa geru valdymu“ (Quarantelli, 1993, p. 30). Nepaisant to, kad tokie planai gali būti kokybiškai parengti, vis dėlto didžioji dalis veiksmų ekstremaliosios situacijos metu priklauso nuo vyraujančio rizikos suvokimo. Siekiant to išvengti svarbu orientuotis ne tik į plano, kaip elgtis ekstremaliųjų situacijų metu, parengimą, bet ir stengtis tą planą praktiškai patikrinti. Todėl kai planas yra parengtas jis turi būti įgyvendinamas. Šis procesas, anot R. W. Perry (2004), turėtų prasidėti gebėjimų įvertinimu. Todėl tai sąlygoja perėjimą prie mokymų bei pratybų.

Planas tai neišvengiama pasirengimo dalis nusakanti veiksmus ekstremaliosios situacijos eigoje ir po jos. Kiekviena organizacija, o ypač tos, kurios vykdo pavojingas veiklas privalo turėti planą, užtikrinantį pasiruošimą ekstremaliosioms situacijoms. Nenutrūkstamą organizacijos veiklą padės užtikrinti tęstinės veiklos planas, kurio dėka yra įvertinamos galimos rizikos ir jų poveikis organizacijos veiklai. Tačiau net ir tinkamai parengtas planas nebūtinai bus veiksmingas, jei nebus praktiškai patikrintas mokymų ir pratybų metu. Kadangi planavimas yra tęstinis procesas, vykstantis nuolat, todėl esant kokiems nors pokyčiams planą reikia papildyti ar pakeisti nauju.

2.2.2. Pasiruošimo proceso mokymų organizavimas darbuotojams

Pasiruošimo metu svarbu dėmesio skirti ne tik planų rengimui, bet taip pat personalui. Nekvalifikuoti, žinių bei patirties stoka pasižymintys darbuotojai ekstremaliosios situacijos metu negalės tinkamai atlikti veiksmų nurodytų tęstinės veiklos plane. Organizacija privalo skirti dėmesio darbuotojų apmokymui ir pratyboms, kad nurodytų jų pareigas bei atsakomybę.

Mokymų svarba yra grindžiama tuo, kad tęstinės veiklos planas yra įtvirtinamas organizacijos kultūroje ir vėliau tampa neatskiriama jos dalimi. Betty A. Kildow (2011) pažymi, kad, jei darbuotojai nėra informuoti apie tokių planų egzistavimą ir nedalyvauja praktiškai patikrinant plano veiksmingumą, tokiu atveju remiantis jų suvokimu, tokių planų išvis nėra. Todėl kiekvienas darbuotojas turi būti informuotas apie savo veiksmus ekstremaliosios situacijos metu, organizacijos pareigas darbuotojų atžvilgiu, tarpusavio komunikavimo ir bendradarbiavimo procedūras. Tai yra ypač svarbu, kadangi nesant informuotiems galima pridaryti papildomos žalos.

Apmokymai tai svarbi pasiruošimo dalis, kuri yra glaudžiai susijusi su plano rengimu. W. Jacko Duncano ir kt. (2011) nuomone, rašytinis planas neturi galios tol, kol nėra patikrinamas ir kol visi darbuotojai su juo nesupažindinami. Vadinasi, svarbu yra atlikti mokymus, kad kiekvienas žinotų, kokios yra jo pareigos įvykus ekstremaliajai situacijai, o pratybų dėka patikrinti plano veiksmingumą ir įsitikinti, kad yra žinoma kaip panaudoti turimus įgūdžius ir žinias praktiškai. Mokymai taip pat prisideda prie tęstinės veiklos plano tobulino, kadangi jų metu yra gaunamas grįžtamasis ryšis, kuris atskleidžia esamas klaidas ar spragas (Perry, 2004). Šis procesas turi užtikrinti tinkamą veikimą įvykus nelaimei. Tačiau dėmesys atkreiptinas ir į tai, kad mokymų metu yra orientuojamasi ne tik į dalyvių, t.y. darbuotojų turimų žinių, gebėjimų bei patirties patikrinimą, bet ir į šių kompetencijų suteikimą ir stiprinimą (Moore, Lakha, 2006). Remiantis autorių pozicijomis, teigtina, kad apmokymai turi dvejopą naudą, t.y. patikrinamas rašytinio plano veiksmingumas ir suteikiamos bei tobulinamos kompetencijos.

Neapmokyti darbuotojai gali tapti grėsmės šaltiniu ir tokiu būdu prisidėti prie ekstremaliosios situacijos išplitimo, o ne jos valdymo. Tokiu atveju net ir turimi geri paruošiamieji planai nepadės sumažinti padarinių poveikio, jei personalas nėra paruoštas veikti grėsmės atveju. J. Rutherford (2008) manymu, personalas netinkamai veikia, nes nesupranta savo pareigų, neturi patirties bei nesugeba atlikti jiems paskirto darbo. Kadangi mokymai tai veikla, kurios metu informacija pateikta plane yra aiškiai perteikiama respondentams (Perry, 2004), todėl, mokymų paskirtis ir yra užtikrinti, kad visi ne tik žinotų, bet ir galėtų atlikti jiems priskirtas pareigas ir atsakomybę. Būtent todėl, mokymai turėtų tapti neatskiriama plano dalimi.

Dar viena priežastis, kodėl mokymas yra svarbus yra ta, kad šis procesas „sumažina jautrumą krizėms ir padeda įgyvendinti paskirtą pareigą“ ekstremaliųjų situacijų metu (Rutherford, 2008, p.

137). Tai reiškia, kad mokymų procesas įtvirtina žinojimą, ką darbuotojai privalo atlikti ir sustiprina susitelkimą ties savo pareigų atlikimu ir jiems priskirta atsakomybe. Todėl ekstremaliųjų situacijų metu jie neturėtų pasimesti, o atliekami veiksmai bus pažįstami.

Mokymai tai pasiruošimo dalis skirta patobulinti veiksmus ekstremaliųjų situacijų metu, kuri privalo būti kruopščiai suplanuota. Mokymo proceso metu yra išsiaiškinamos kiekvieno dalyvio pareigos, patikrinami turimi gebėjimai ir žinios, bei suteikiami nauji. Be to, ši veikla yra tarsi tęstinės veiklos plano patikrinimas, nes prisideda prie jo tobulinimo. Nors suteiktos teorinės žinios ir įgūdžiai yra naudingi, tačiau siekiant įtvirtinti mokymų metu įgautas žinias patartina į planavimo procesą įtraukti ir pratybas.

2.2.3. Plano veiksmingumo patikrinimas

Sukurto plano veiksmingumas privalo būti patikrintas praktiškai. Pagrindinė plano patikrinimo užduotis yra įsitikinti, kad tęstinės veiklos planas yra tinkamas įveikti numatytas rizikas. Testavimo metu yra vykdomos pratybos, kurių paskirtis yra ne tik patikrinti plano tinkamumą, bet ir užtikrinti, kad darbuotojai žinotų savo pareigas, jų dėka yra suteikiama pasitikėjimo ir sumažinama galimybė atsirasti panikai. Ši sritis yra be galo svarbi, kadangi esant planui, bet nesant pratyboms, t.y. neatliekant plano patikrinimo yra galimybė patirti nuostolius (Cerullo, Cerullo, 2004). Išsamus patikrinimas suteiks pasitikėjimo ir galimybę atsigauti po ekstremaliosios situacijos. Pasak autorių, organizacija neturinti tokio plano turi mažas galimybes atsigauti po susiklosčiusios situacijos.

Pratybos kaip ir plano sudarymas bei mokymai atlieka svarbų vaidmenį pasiruošimo procese. Jų metu atsiranda galimybė patikrinti kaip rašytiniai planai ir įvykdyti mokymai bus įgyvendinti įvykus ekstremaliajai situacijai, kitaip tariant pratybos kaip ir mokymas atspindi organizacijos pasiruošimą.

Pratybos tai „veikla, kuri skatina patikrinti procedūras ir užtikrina dalyvių praktiką jiems paskirtuose vaidmenyse“ (CDEM exercises, 2009, p. 7). Siekiant geriau įsisavinti praeitus mokymus būtinos yra pratybos, kurios pagerina išteklių naudojimą, tarpusavio bendradarbiavimą. Pratybos suteikia galimybę patikrinti savo gebėjimus iki įvykstant ekstremaliajam įvykiui. Tačiau, anot Edwardo P. Borodziczo (2005), pratybos bus veiksmingos tik tada, kai dalyvaujantieji žinos pratybų ir savo dalyvavimo tikslą. Priešingu atveju pratybos nebus veiksmingos.

R. W. Perry (2004) manymu, pratybos gali būti taikomos kaip mokymo forma, treniruotė prieš ekstremaliąją situaciją. Tokių pratybų kaip ir mokymų metu išryškėja galimi plano trūkumai, kurie gali būti tobulinami. Manytina, kad pratybų metu išryškėja ne tik darbuotojų gebėjimai ir galimybės veikti ekstremaliojoje situacijoje, bet ir tai, kaip darbuotojai suvokia riziką ir kokios gali išryškėti grėsmės pasekmės (Borodzicz, 2005). Kadangi pratybos atspindi kaip mokymų metu yra įsisavintos žinios, todėl svarbu, kad šie du procesai būtų tarpusavyje suderinti.

Atliekamos pratybos turi būti realistiškos ir atspindėti didesnę įvykio atsiradimo tikimybę. Pratybų metu svarbu stebėti kaip kiekvienas narys vykdo jam paskirtas funkcijas, žymėtis pastabas. Vėliau patartina aptarti įvykusias pratybas ir sužymėtas pastabas, kaip antai, kodėl kažkas nevyko pagal planą (Kildow, 2011). Tai yra naudinga, kadangi šiomis pastabomis galima pasinaudoti tobulinant planą.

Atkreiptinas dėmesys, kad pratybos palyginus su mokymo procesu apima platesnį spektrą veiksmų, kadangi į jas įeina ne tik asmeninių kompetencijų patikrinimas, bet ir organizacijos, grupių veiksmai ir gebėjimas veikti krizės metu, naudojamos įrangos patikimumo patikrinimas (Moore, Lakha, 2006; Borodzicz, 2005), taip pat vertinamos galimybės valdyti situaciją pratybų metu. Šio proceso metu yra koncentruojamasi į fizinę organizacijos parengtį.

Danny M. Petersono ir R. W. Perry (1999) atliktų tyrimų duomenimis dalyvavimas pratybose daro poveikį grėsmės rizikos suvokimui. Pratybos pakeičia dalyvaujančių darbo komandoje ir darbo rizikos suvokimą, reagavimo tinklų veiklos veiksmingumą bei pratybų pakankamumą. Mokymų ir pratybų derinys sumažina suvokiamos rizikos lygį tuo atveju, kai pratybos yra pavykusios ir pateikia teigiamą rezultatą. Dalyvaujantieji patys gali įvertinti gresiantį pavojų, nustatyti kaip pasikeitė anksčiau jų suvokiama rizika ir kaip ji suvokiama po pratybų.

Siekiant pasiruošti ekstremaliųjų situacijų valdymui yra siūlomas vienas iš būdų, padėsiančių suvokti kaip bendruomenė suvokia tam tikras grėsmes, t.y. pateikti grėsmių scenarijus. Šių scenarijų dėka bus išsiaiškinta kaip yra suvokiamos grėsmės bei padės suformuluoti rizikos mažinimo strategijas ir tokiu būdu pasiruošti ekstremaliosioms situacijoms (Paton, Johnston, 2001). Toks pats scenarijų metodas gali būti taikomas organizacijoje imituojant ekstremaliąsias situacijas. Šių sukurtų scenarijų patikimumas gali būti tikrinamas mokymų ir pratybų metu (Jackson ir kt., 2011). Tokio pobūdžio pratybos tai ne tik galimybė patikrinti darbuotojų gebėjimus, jų elgesį ekstremaliosios situacijos metu, bet ir reikalingos įrangos veikimą.

Pratybos kaip ir mokymai yra svarbi pasirengimo ekstremaliosioms situacijoms plano dalis. Pratybos leidžia įvertinti bendrą organizacijos pasiruošimą, dalyvių ar atskirų skyrių tarpusavio veiksmų suderinamumą ir gebėjimą bei mokėjimą dirbti kartu su kitais nariais ar skyriais. Svarbu yra tai, kad pratybų metu atlikti plane numatyti veiksmai suteikia galimybę įžvelgti klaidas ir jas pataisyti, tokiu būdu prisidedant prie plano tobulinimo ir geresnio pasiruošimo.

3. RIZIKOS SUVOKIMO ĮTAKA INFORMACINIŲ TECHNOLOGIJŲ ORGANIZACIJOS VEIKLAI

3.1. Tyrimo metodika ir organizavimas

Siekiant nustatyti kokį poveikį rizikos suvokimas daro IT organizacijos pasiruošimui ekstremaliosioms situacijoms buvo pasirinkta atlikti kiekybinį tyrimą. Šio empirinio tyrimo pasirinkimą lėmė tai, kad gautų kiekybinių duomenų dėka galima bus patvirtinti ar paneigti iškeltas hipotezes.

Tyrimo metu buvo patikrintos iškeltos šios hipotezės:

H_1: IT organizacijos darbuotojai kaip didžiausią poveikį turinčias organizacijos veiklai išskiria technologines grėsmes.

H_2: tiriama organizacija neturi plano aprašančio pasiruošimo veiksmus ekstremaliosioms situacijoms.

H_3: respondentai neįžvelgia tęstinės veiklos plano poreikio savo organizacijai.

Kiekybiniam tyrimui yra būdinga tai, kad duomenys yra pateikiami skaitmenine išraiška ir yra galimybė nustatyti statistinius ryšius tarp įvairių kintamųjų. Kadangi tyrimo metu siekiama patvirtinti arba paneigti iškeltas hipotezes, todėl šis metodas yra laikomas tinkamiausiu ir patikimiausiu (Pruskus, 2003; Kardelis, 2007; Priest, 2010).

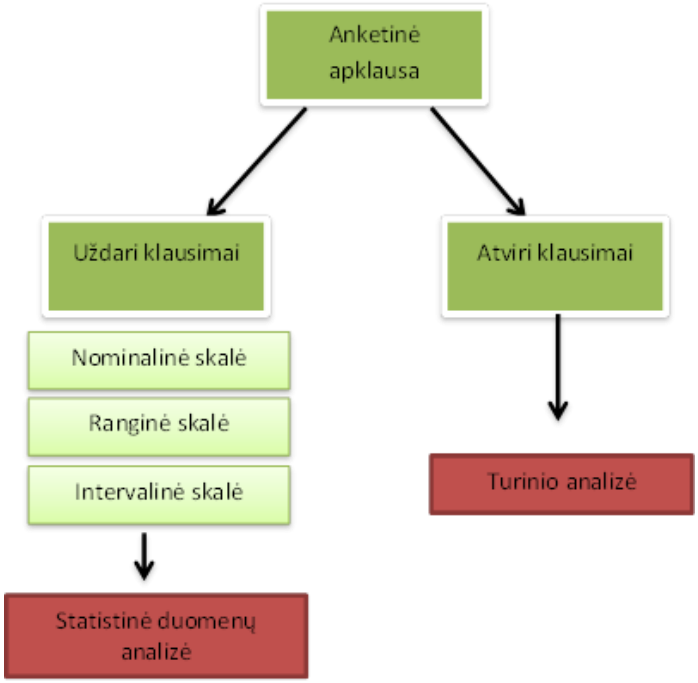
Tyrimo ***instrumentarijumi*** buvo pasirinkta anketinė apklausa. Anketinė apklausa tai metodas, kuris įgalina duomenų rinkimą naudojant klausimyną, skirtą respondentui. Anketos ypatumas yra tas, kad yra pateikiami tiek uždari, tiek atviri, tiek pusiau uždari klausimai į kuriuos gali būti atsakoma raštu arba žodžiu. Pateikiant anketą siekiama kuo nuodugniau pažinti tiriamąjį reiškinį (Guščinskienė, 2004). Anketinė apklausa buvo pasirinkta, kadangi (Tidikis, 2003):

- ✓ padeda išryškinti klausimo esmę,
- ✓ pasižymi objektyvumu, kadangi atsakantysis yra orientuojamas į daugumos priimtinus atsakymus,
- ✓ yra lengviau interpretuoti atsakymus.

Anketinę apklausą tinka taikyti tada, kai tiriama problema nėra pakankamai išanalizuota, todėl siekiama ištirti socialinį reiškinį, o tyrimo dalyku tampa asmens įsitikinimai, vertybės, poreikiai ar interesai (Didžiulienė, 2004). Šis metodas yra tinkamas, nes siekiama išsiaiškinti, kaip darbuotojai suvokia riziką ir kaip tai veikia organizacijos pasiruošimą ekstremaliosioms situacijoms.

Respondentams buvo pateiktos dviejų tipų anketos (7 pav.). Atliekant žvalgomąjį tyrimą respondentams buvo pateikta anketa (žr. 1 priedą) apimanti atvirus klausimus. Žvalgomasis tyrimas

buvo atliktas siekiant susidaryti bendrą vaizdą apie esamą organizacijos situaciją bei tapo pagalbiniu įrankiu sudarant antrą anketą. Taip pat jis tapo naudingu, nes suteikė nemažai naudingos informacijos bei papildė antros anketos gautus duomenis.



7 pav. **Anketinės apklausos schema**

Anketą (žr. 2 priedą) sudarė įvadinė ir pagrindinė dalys. Įvadinėje dalyje respondentai buvo supažindinti su tyrimo atlikimo tikslu, duomenų panaudojimu ir anonimiškumo užtikrinimu. Taip pat buvo pateiktos anketoje vartojamos sąvokos.

Pagrindinę anketos dalį sudarė pateiktas trijų kategorijų, klausimynas, kuriame iš 18 klausimų buvo pateikta 16 uždarų ir 3 pusiau uždari klausimai. Pateikiant uždarus klausimus buvo suformuluoti galimi atsakymų variantai. Pirmą klausimų kategoriją sudarė *pavojų organizacijos veiklai vertinimas*, į antrą kategoriją įėjo *saugumo užtikrinimo apmokymai, aprūpinimas įranga*, o trečią kategoriją sudarė klausimai apie *tęstinės veiklos planavimą*. Šių klausimų kategorijos buvo sudarytos su tikslu išsiaiškinti:

- ✓ kokias rizikas įžvelgia organizacijos darbuotojai,
- ✓ kaip jie vertina savo organizacijos pasiruošimą ekstremaliosioms situacijoms,
- ✓ kokias priemones organizacija taiko pasiruošimo srityje.

Prieš atliekant apklausą svarbu nustatyti ***tyrimo imtį***. Šis žingsnis, anot K. Kardelio (2007), yra ypač svarbus, jei norima padaryti statistiškai reikšmingas išvadas. Imčiai sudaryti buvo pasirinkta tikimybinė atranka. Siekiant nustatyti respondentų skaičių svarbu žinoti, kad tiriamos informacinių technologijų organizacijos generalinę visumą sudaro 81 darbuotojas.

Imties dydžiui nustatyti buvo remiamasi Paniotto formule (Valackienė, 2004):

$$n = \frac{1}{\Delta^2 + \frac{1}{N}}$$

Čia:

n – atvejų skaičius atrankinėje grupėje

N – generalinė aibė

Δ - paklaidos dydis

Vadinasi, remiantis atliktais apskaičiavimais atvejų skaičių atrankinėje grupėje sudaro 67 respondentai.

Surinktiems duomenims apdoroti ir pateikti išvadas būtina pasirinkti tinkamą metodą. Tinkamiausias būdas kiekybinei analizei atlikti ir nustatyti ryšį tarp kintamųjų yra taikyti statistikos programų paketą (SPSS Statistics 17.0) (Luobikienė, 2006). Kadangi žvalgybinio tyrimo metu buvo gauta žodinė informacija, nuspręsta duomenų analizę atlikti remiantis kokybine turinio analize *(angl. content analysis)*. Ši analizė pasižymi tuo, kad surinkta informacija yra interpretuojama atsižvelgiant į išskirtas šios analizės metu kategorijas (Bitinas, 2008).

Atliekant kokybinę turinio analizę turimas tekstas, šiuo atveju respondentų pasisakymai, buvo skaidomi į kelias kategorijas. Visų pirma analizuojant apklaustųjų pasisakymus buvo išskiriami analitiniai turinio vienetai (žr. 3 priedą). Tada respondentų pasisakymams buvo suteikiami kodai (Berg, 2007) arba kitaip etiketės (Bitinas, 2008), t.y. išskiriamos potemės ir temos geriausiai apibūdinančios pasisakančiojo žodžius.

Prie kiekvienos iš potemių buvo pridedami pavyzdžiai iš respondentų atsakymų į pateiktus jiems klausimus. Pasirinktų etikečių dėka galima paprasčiau identifikuoti, susisteminti ir atrasti turimus duomenis. Duomenys buvo rūšiuojami pagal išskirtas kategorijas, buvo identifikuojamos panašios frazės, nustatomi tarpusavio ryšiai. Atlikus šiuos veiksmus buvo sudaromos stambesnės kategorijos, t.y. išskiriamos temos arba kitaip apibendrinamoji frazė (Berg, 2007; Bitinas, 2008).

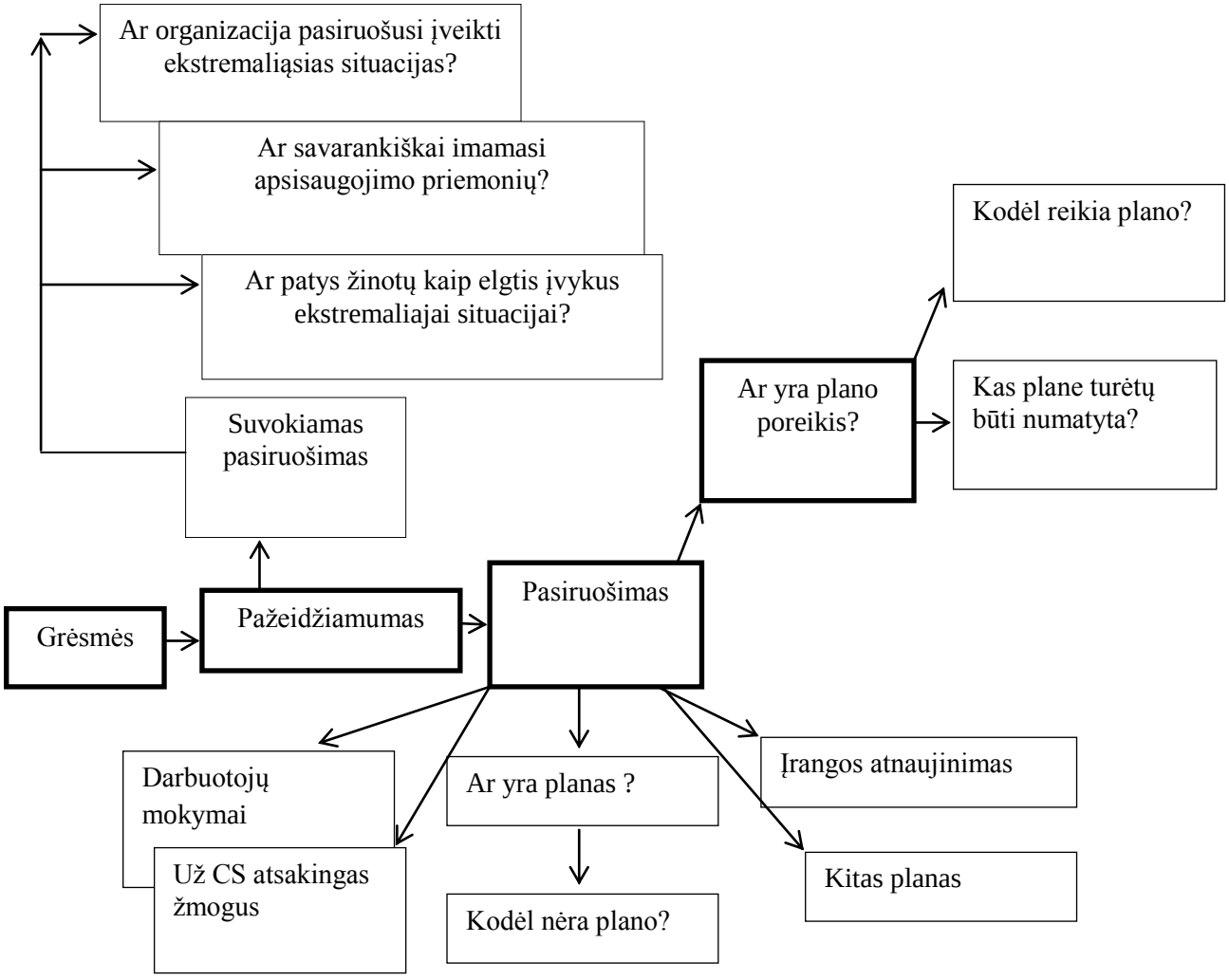
Siekiant geriau pamatyti atliktos analizės rezultatus, apdoroti duomenys buvo pavaizduoti lentelėje. Atlikus duomenų analizę darbo pabaigoje yra pateikiamos atlikto tyrimo išvados.

Tyrimo etika. Tyrimui atlikti buvo prašoma leidimo organizacijos vadovų. Nurodžius planuojamo atlikti tyrimo tikslą bei uždavinius buvo gautas sutikimas apklausti tiriamuosius. Dalyvavimas apklausoje buvo grindžiamas laisvanoriškumo principu (Rupšienė, 2007). Nepanorę dalyvauti apklausoje galėjo atsisakyti. Tiriamieji buvo informuoti apie tyrimo atlikimo tikslą, anonimiškumo bei konfidencialumo užtikrinimą. Siekiant užtikrinti anonimiškumą atsakant į žvalgomojo tyrimo klausimus, atviro tipo anketa buvo siunčiama vienam už anketų platinimą atsakingam organizacijos darbuotojui elektroniniu paštu, o vėliau tas pats asmuo visas anketas persiuntė atgal. Atliekant anketinį tyrimą, dalis anketų, pateikiant elektroninę nuorodą į internetinės

svetainės tinklapį http://www.manoapklausa.lt/, buvo išsiųsta el. paštu, kita dalis – buvo pateikta nunešant atspausdintas anketas į organizaciją.

3.2. Tyrimo rezultatų analizė

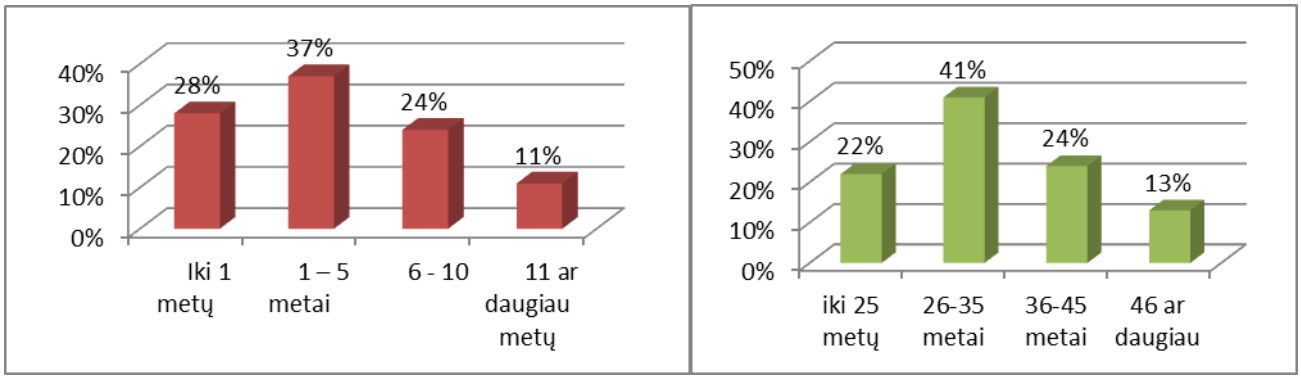
Siekiant nuoseklumo visi klausimai buvo analizuojami pagal anksčiau sudarytą schemą (8 pav.).



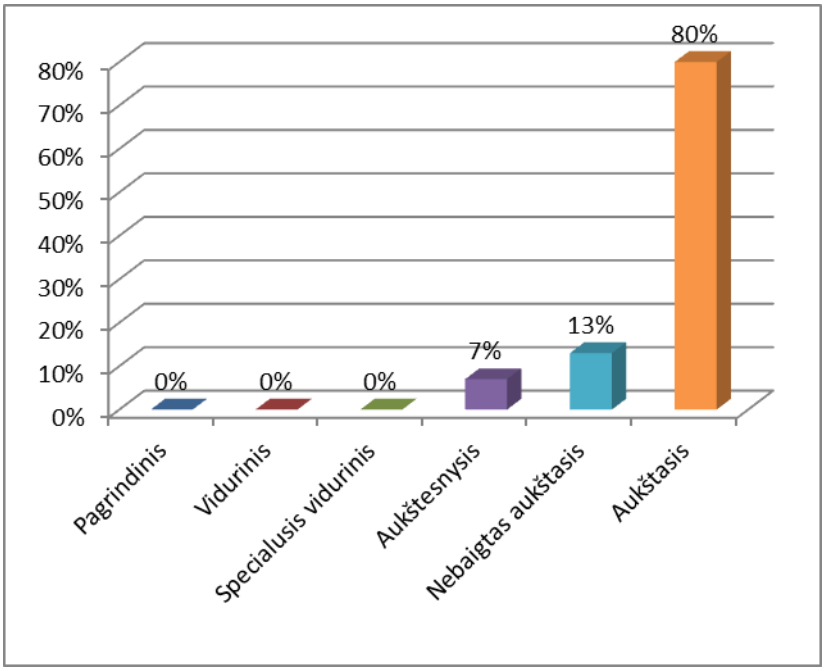
8 pav**. Klausimų analizės schema**

Tyrimas atliktas nedidelėje iš 81 žmogaus susidedančioje IT organizacijoje. Iš 67 respondentų, kuriuos reikėjo apklausti į anketas atsakė 46. Atsižvelgiant į mažą atsakomumą galima daryti prielaidą, kad darbuotojai nebuvo suinteresuoti dalyvauti vykdomame tyrime.

Daugumos (41 proc.) respondentų amžius yra gan jaunas, t.y. siekia 26 – 35 metus, todėl ir darbo patirtis (9 pav.) tiriamoje organizacijoje nėra didelė 1 – 5 metai (37 proc.). Iš visų dalyvavusių apklausoje 80 proc. turi aukštąjį išsilavinimą (10 pav.).



9 pav. **Respondentų darbo patirtis organizacijoje ir amžius**



10 pav. **Respondentų išsilavinimas**

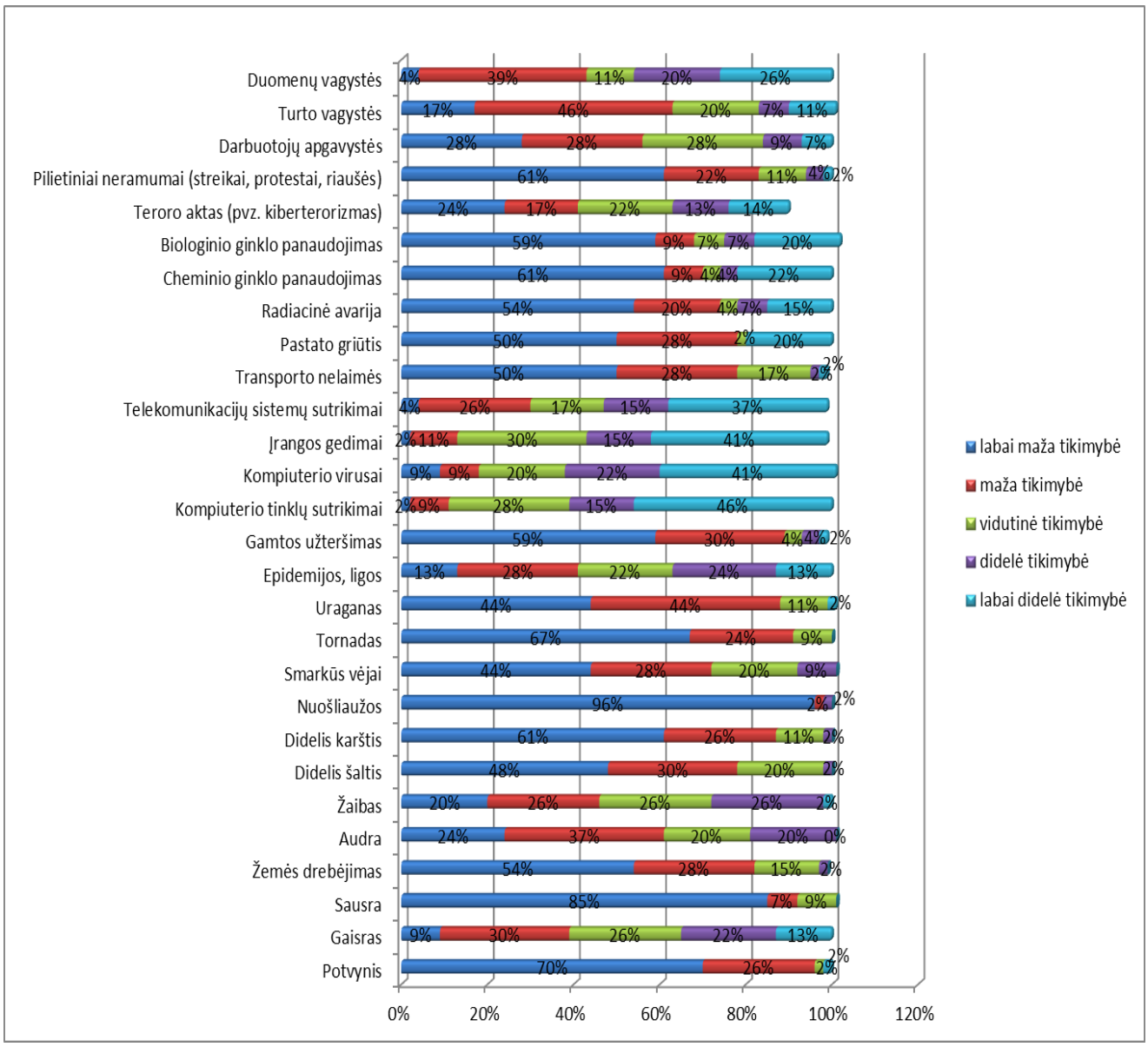
Pirmiausia yra analizuojamos respondentų išskirtos grėsmės, galinčios turėti poveikį organizacijos veiklai. Atlikto žvalgybinio tyrimo (žr. 5 priedą) metu respondentai išskyrė technologines grėsmes, darančias poveikį organizacijos veiklai. Atlikus anketinę apklausą ir pateikus platų grėsmių pasirinkimą, didžioji dalis respondentų vis tiek pasirinko technologines grėsmes (11 pav.) kaip turinčias didžiausią poveikį organizacijos veiklai.

Kaip labai didelės ir didelės tikimybės grėsmes respondentai išskyrė kompiuterio virusus (atitinkamai 41 proc. ir 22 proc.). Labai dideles ir vidutines tikimybes įžvelgė: kompiuterio tinklų sutrikimuose (46 proc. ir 28 proc.), įrangos gedimuose (41 proc. ir 30 proc.), o kaip labai dideles bei mažas tikimybes įvardijo telekomunikacijų sistemų sutrikimus (37 proc. ir 26 proc.).

Žmogaus sukurtos grėsmės tokios kaip turto (46 proc.) ar duomenų vagystės (39 proc.), buvo įvertintos kaip mažą tikimybę turinčios. Anot respondentų, įvykę pilietiniai streikai (61 proc.) turėtų labai mažą poveikį organizacijos veiklai.

Respondentai mažą tikimybės laipsnį suteikė ir gamtinėms grėsmėms. Jų manymu, jos mažiausiai galėtų paveikti jų vykdomą veiklą. Daugiausia toks grėsmių išskyrimas buvo nulemtas turima patirtimi (žr. 5 priedą). Atsižvelgiant į tokį respondentų atsakymų pasiskirstymą darytina prielaida, jog viena vertus respondentai pasirinko tokias grėsmes, kurios tiesiogiai daro įtaką jų darbui, kita vertus organizacijos darbuotojai nesuvokia, kad ne tik technologinės, bet ir kitokio pobūdžio grėsmės, įvykusios ekstremaliosios situacijos taip pat gali paveikti organizacijos veiklą.

Remiantis tyrimo duomenimis galima patvirtinti iškeltą pirmą hipotezę, kad IT organizacijos darbuotojai kaip didžiausią poveikį turinčias organizacijos veiklai išskiria technologines grėsmes.



11 pav. **Grėsmių išskyrimas**

Išsiaiškinus, kokios grėsmės gali turėti poveikio organizacijos veiklai, respondentų buvo klausiama ar organizacija yra pažeidžiama, jei taip kokiuose srityse ir kodėl.

Klausiant kodėl, jų nuomone, organizacija yra pažeidžiama, respondentai pripažino, kad kaip ir bet kokia kita organizacija ji taip pat gali susidurti su grėsmėmis. Tačiau kaip pagrindinė pažeidžiamumo priežastis buvo įvardinta vykdoma veikla, kuri yra susijusi su IT (2 lent.).

2 lentelė. Požiūris į organizacijos pažeidžiamumą

Respondentų pasisakymai	Potemė	Tema
Taip, kiekviena organizacija yra pažeidžiama ir jautri grėsmėms, mūsų įmonė – ne išimtis (A7-7)	Organizacijos pažeidžiamumo prilyginimas kitoms organizacijoms	Lygiavimasis į kitas organizacijas
Visos organizacijos yra pažeidžiamos ir jautrios. Vienos mažiau, kitos daugiau (C7-8)		

2 lentelės tęsinys kitame puslapyje

2 lentelės tęsinys

Respondentų pasisakymai	Potemė	Tema
Pažeidžiama. Pažeidžiami netgi bankai turintys prevencijos skyrius su keletu ar keliolika darbuotojų (G7-6)	Organizacijos pažeidžiamumo prilyginimas kitoms organizacijoms	Lygiavimasis į kitas organizacijas
Nepažeidžiama, tačiau visko gali nutikti (B7-7)	Galimybės susidurti su grėsmėmis numatymas	Savisaugos priemonės
Jautri, tačiau nepažeidžiama, nes turim planą, kuriuo vadovaujantis grėsmių tikimybė minimali (I7-6)	Apsaugos nuo grėsmių planas	
Nei viena organizacija nėra apsaugota nuo grėsmių, tačiau kiekviena stengiasi, kad tos grėsmės neįvyktų (J7-7)	Pastangos apsisaugoti nuo grėsmių	
Organizacija yra rinkos dalis, todėl pokyčiai rinkoje įtakoja organizaciją (D7-10)	Išorinių veiksnių įtaka organizacijos veiklai	Priežastys sąlygojančios organizacijos pažeidžiamumą
Organizacija turi santykinę apsaugą nuo kai kurių grėsmių, bet ne nuo visų įmanomų tam, kad išlaikytų status quo (D7-11)	Santykinis organizacijos apsaugos buvimas	
Kai kurioms grėsmėms jautri (E7-7)		
Ir taip ir ne. Esant dideliam norui bet kokios organizacijos apsaugas šiais laikais galima, jeigu ne neutralizuoti, bet bent sustabdyti įmonės darbą (K7-8)		
Galima (vadinti pažeidžiama), nes kol kas nevaldome proceso (L7-7)	Proceso nevaldymas	
Manau, kad bendrovė yra pažeidžiama atsižvelgiant į teikiamų paslaugų pobūdį (F7-9)	Paslaugų specifika	
Taip. Didžioji dalis darbų vykdoma virtualioje erdvėje, todėl bet koks sutrikimas stabdo darbą, prarandama informacija ar net tam tikro laikotarpio darbo rezultatai (H7-7)		

Organizacijos darbuotojai (A7-7; C7-8; G7-6) sutaria, kad ši organizacija kaip ir bet kokia kita nėra visiškai apsaugota nuo galimų grėsmių ir todėl yra pažeidžiama, vis dėlto yra dedamos pastangos toms grėsmėms sumažinti. Organizacija numato, kad yra galimybė įvairioms grėsmėms atsirasti, todėl kaip teigia vienas iš apklaustųjų „(...) turim planą, kuriuo vadovaujantis grėsmių tikimybė minimali“ (I7-6). Tačiau, kaip buvo išsiaiškinta vėliau (žr. 4 lent.), klausimas dėl plano yra abejotinas.

Nepaisant to, kad yra veiksnių, nusakančių organizacijos rūpinimąsi savo apsauga, vis dėlto juos nusveria nemažai priežasčių sąlygojančių jos pažeidžiamumą.

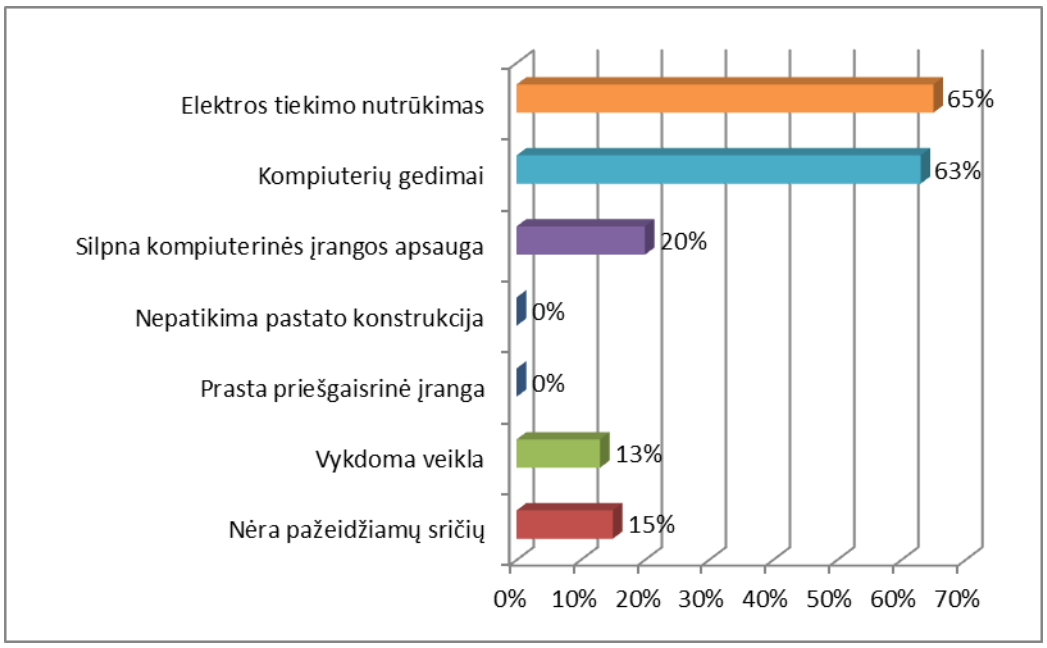
Respondentų manymu, pirmiausia organizacijos pažeidžiamumą įvairioms grėsmėms sąlygoja santykinė organizacijos apsauga nuo grėsmių. Tai reiškia, kad organizacija taiko apsaugos priemones, tačiau jos nėra orientuotos į visas galimas grėsmes (D7-11; E7-7; K7-8). Be to, toks santykinis apsaugų taikymas gali pakenkti organizacijos darbui. Anot vieno respondento (K7-8), „(...) organizacijos apsaugas (...) galima, jeigu ne neutralizuoti, bet bent sustabdyti įmonės darbą.“ Patys darbuotojai pripažįsta, kad pažeidžiamumas atsiranda, kadangi „(...) kol kas nevaldome proceso“ (L7-7).

Visų antra organizacijos darbo specifika, t.y. darbas, kuris vykdomas virtualioje aplinkoje (H7-5), taip pat yra viena iš priežasčių, nulemiančių jos pažeidžiamumą. Pažeidžiamumas yra pripažįstamas, kadangi yra rizika prarasti sukauptus duomenis, o taip pat „bet koks sutrikimas stabdo darbą, prarandama informacija ar net tam tikro laikotarpio darbo rezultatai“ (H7-7). Būtent dėl šios priežasties organizacija turėtų skirti dėmesį pasiruošimui skirtam apsisaugoti nuo grėsmių ekstremaliųjų situacijų metu.

Visų trečia, organizacija yra veikiama išorinių veiksnių, kurie turi poveikio jos tolimesnei veiklai. Kadangi organizacija yra „rinkos dalis“ (D7-10), todėl kaip pastebi respondentas joje vykstantys pokyčiai turi įtakos organizacijai.

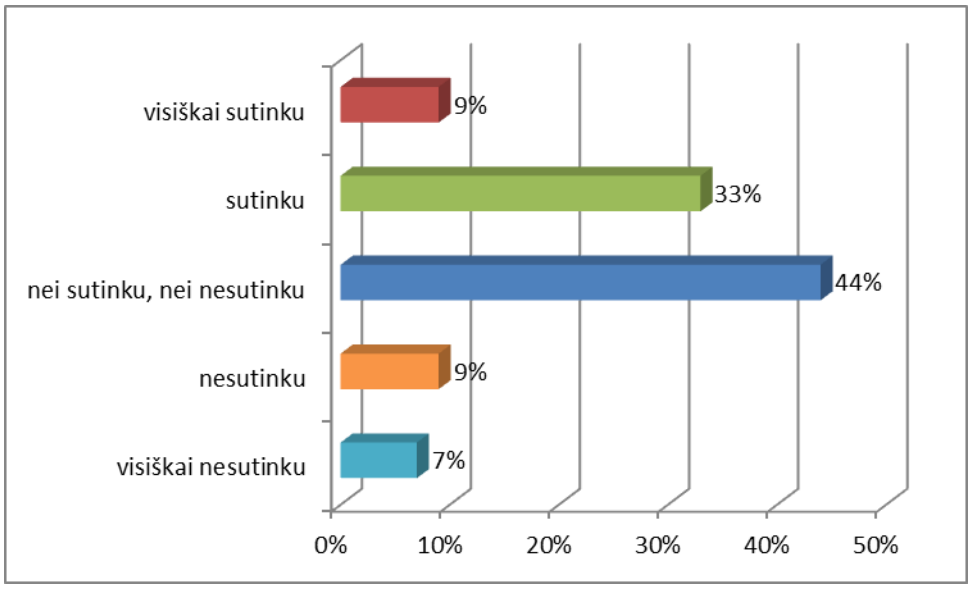
Kaip pažeidžiamiausias organizacijos sritis (12 pav.) net 65 proc. respondentų pasirinko elektros tiekimo nutrūkimą ir 63 proc. pasirinko kompiuterių gedimus. Kiti (13 proc.) kaip pažeidžiamą sritį įvardino vykdomą veiklą, t.y. darbas informacinių technologijų srityje teikiant programavimo paslaugas. Nei vienas iš apklaustųjų neįvardino prastos priešgaisrinės įrangos ar nepatikimos pastato konstrukcijos kaip pažeidžiamos organizacijos srities. Daugiau nei įvertinusių vykdomą veiklą, t.y. 15 proc. respondentų nuomone, organizacijoje išvis nėra pažeidžiamų sričių. Tikėtina, kad dėl tokio požiūrio, kai nėra pastebima jokių pažeidžiamų sričių, nebus nuspręsta imtis jokių apsaugos, pasiruošimo ekstremaliosioms situacijoms priemonių, nes paprasčiausiai nebus įžvelgiamas toks poreikis.

Kaip rodo apklausos rezultatai labiausiai pažeidžiamumas yra pastebimas srityse, kurios yra tiesiogiai susijusios su organizacijos veikla. Tai, kad vien dėl savo vykdomos veiklos organizaciją galima vadinti esant pažeidžiama, pripažino daugelis respondentų.



12 pav. **Pažeidžiamiausios organizacijos sritys**

Išsiaiškinus, kad yra pažeidžiamų sričių, kyla klausimas ar organizacija imasi veiksmų, kad bent šiek tiek sumažintų savo pažeidžiamumą. Todėl buvo klausiama ar darbuotojų nuomone, organizacija yra pasiruošusi bet kokioms grėsmėms (13 pav.). 44 proc. respondentų abejojo, nes nei sutiko, nei nesutiko su šiuo teiginiu. O 33 proc. sutiko, kad organizacija yra pasiruošusi bet kokioms grėsmėms, todėl jos neturėtų stipriai paveikti jos veiklos. Respondentų, kurie visiškai sutiko ir nesutiko su pateiktu teiginiu, nuomonės pasiskirstė po lygiai (9 proc.). Mažiausiai buvo visiškai nesutinkančių su teiginiu, kad organizacija pasiruošusi bet kokioms grėsmėms.



13 pav. **Organizacijos pasiruošimo bet kokioms grėsmėms įvertinimas**

Žvalgybinio tyrimo metu buvo gauta nemažai informacijos, galinčios papildyti šį nagrinėjamą pasiruošimo grėsmėms klausimą. Paklausus, kodėl respondentų nuomone, organizacija yra pasiruošusi įveikti bet kokias grėsmes buvo įvardijama nemažai priežasčių (3 lent.).

3 lentelė. Organizacijos pasiruošimas įveikti grėsmes

Respondentų pasisakymai	Potemė	Tema
Žinau, nes jau vieną tokią grėsmę įveikėme (A6-6)	Patirtis	Pasiruošimo grėsmėms veiksniai
Organizacija ilgai gyvuoja, todėl turi didelę patirtį. (C6-7)		
Taip. Nes tam yra skirti specialistai, kurie už tai atsakingi. (b6-6)	Pasitikėjimas specialistais	
(...), nes dirba daug specialistų (E6-6)		
Taip, dirba profesionalūs (J6-5)		
Apmokyti darbuotojai (J6-6)		
Nežinau. Apie tokius dalykus informacija nėra skleidžiama organizacijos viduje tarp darbuotojų (D6-9)	Informacijos stoka	
Nežinau (G6- 5)		
Neturiu informacijos apie panašaus plano buvimą (H6-6)		
Taip, nes kiekviena solidi įmonė rūpinasi savo reputacija (F6-7)	Rūpinimasis organizacijos veikla	
Rūpinasi veiklos tęstinumo užtikrinimas net ekstremaliomis aplinkybėmis(F6-8)		
Taip, kadangi organizacija įdėjus daug pastangų, jog šios grėsmės neįvyktų (I6-5)		

Kai kurie respondentai įvardino sukauptą organizacijos patirtį kaip vieną iš pasiruošimo veiksnių. Tą patvirtina respondento pasakymas, kad „organizacija ilgai gyvuoja, todėl turi didelę patirtį“ (C6-7), o taip pat patirtis sukaupta įveikiant susidariusias grėsmes (A6-6). Nors turima patirtis yra svarbus aspektas vertinant susidūrimą su galimomis grėsmėmis, vis dėlto įvykus ekstremaliajai situacijai gali pasireikšti ne tik jau žinomos, bet ir naujos grėsmės. Todėl nereikėtų pasikliauti vien sukaupta patirtimi.

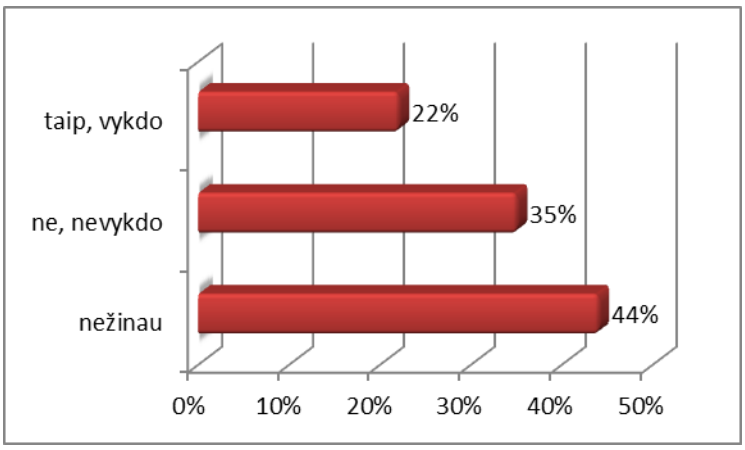
Kalbant apie pasiruošimą taip pat buvo įvardijamas pasitikėjimas specialistais. Šiuo atveju atsakomybė už riziką yra perleidžiama nuo savęs kitiems, kadangi yra tikima, kad įvykus ekstremaliajai situacijai viskuo pasirūpins specialistai. Paklausus ar organizacija yra pasiruošusi įveikti bet kokias grėsmes, buvo atsakyta, kad taip, „nes tam yra skirti specialistai, kurie už tai atsakingi“ (B6-6). Kitas respondentas įvardijo specialistų gausą teigdamas, kad „(...) dirba daug specialistų“ (E6-6). Taip pat buvo įvertintos darbuotojų žinios ir jų profesionalumas (J6-5; J6-6). Manytina, kad ne tik

specialistai turėtų būti atsakingi už organizacijos veiklos atkūrimą, bet remiantis bendradarbiavimo principu ir visi kiti organizacijos darbuotojai.

Kitiems respondentams pritrūko informacijos šiuo klausimu. Jie nežinojo ar organizacija yra pakankamai pasiruošusi įveikti įvairias grėsmes ir ar turi tam skirtą planą (G6-5; H6-6). Kitas respondentas teigė, kad „apie tokius dalykus informacija nėra skleidžiama organizacijos viduje tarp darbuotojų“ (D6-9). Dėl šios priežastis, jis taip pat negalėjo įvardinti kaip organizacija yra pasiruošusi ekstremaliosioms situacijoms.

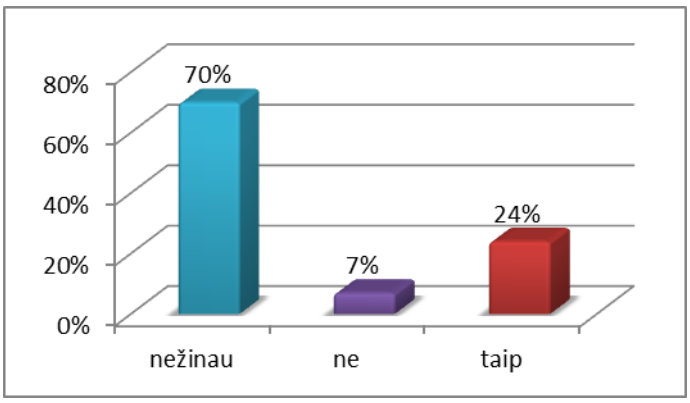
Yra daroma prielaida, kad organizacija rūpindamasi savo įvaizdžiu tuo pačiu rūpinasi ir apsauga nuo grėsmių. Tą patvirtina respondento (F6-7) pasakymas, jog „(...) kiekviena solidi įmonė rūpinasi savo reputacija“ ir „veiklos tęstinumo užtikrinimu net ekstremaliomis aplinkybėmis“ (F6-8). Taip pat yra įžvelgiamos pastangos įveikti grėsmes (I6-5), tačiau kokie konkrečiai tai veiksmai respondentas neįvardijo.

Remiantis pasisakymais, vyrauja suvokimas, kad organizacija yra pasiruošusi įveikti bet kokias grėsmes, tačiau tą galima bus nuspręsti įvertinus ar organizacija turi planą, ar vykdo mokymus, kurių metu yra mokama kokių veiksmų reikėtų imtis, kad būtų galima atkurti organizacijos veiklą po ekstremaliosios situacijos ir, ar reguliariai atnaujina apsisaugojimo priemones. Kadangi dauguma respondentų (44 proc.) pažymėjo, kad nežino ar vyksta mokymai, vadinasi, jie ne tik juose nedalyvavo, bet ir apskirtai neturi informacijos apie jų rengimą (14 pav.).



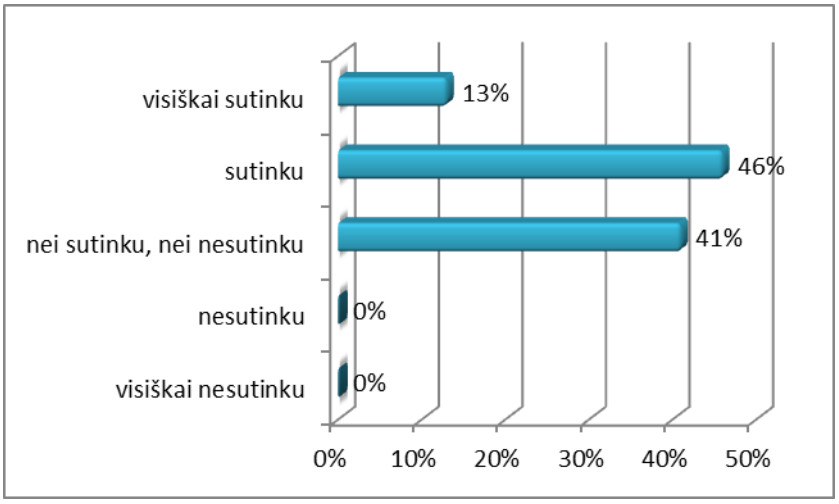
14 pav. **Mokymų padėsiančių plėtoti organizacijos veiklą po ekstremaliosios situacijos vykdymas**

Su panašia situacija susidurta vertinant atliekamą rizikų analizę (15 pav.). Šiuo atveju net 70 proc. respondentų teigė, jog nežino apie tokią analizę, o 24 proc. nurodė, kad vis dėlto rizikų analizė yra vykdoma. Kaip ir analizuojant mokymų rengimą, taip ir vertinant rizikas, pasirodo, kad jei rizikų analizė yra atliekama, tai joje dalyvauja tik dalis darbuotojų.



15 pav. **Organizacijoje vykdoma rizikų analizė**

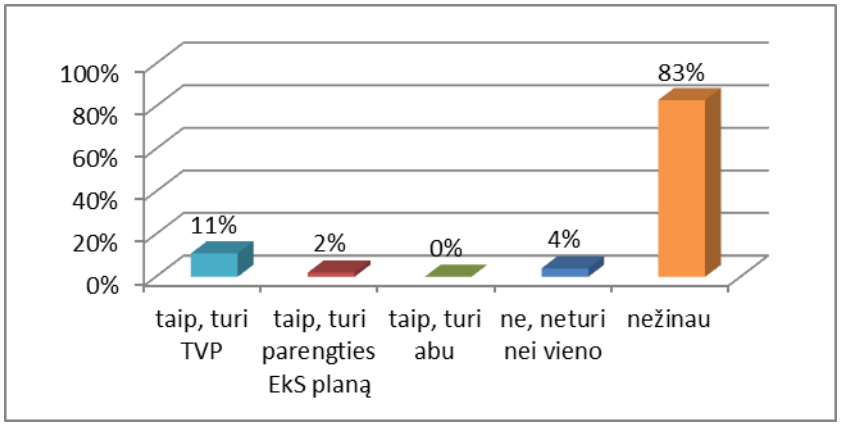
Nagrinėjant įrangos ir kitų apsisaugojimo nuo grėsmių ir ekstremaliųjų situacijų priemonių atnaujinimą paaiškėjo, kad organizacija reguliariai atnaujina turimą įrangą (16 pav.). Iš 46 apklausoje dalyvavusių respondentų 21 (46 proc.) atsakė, kad sutinka su pateiktu teiginiu. 41 proc. respondentų negalėjo atsakyti, ar organizacija atnaujina įrangą ar ne. Nei vienas iš respondentų nepaneigė, kad organizacija atnaujina apsaugos priemones. Vadinasi, darytina išvadą, kad šiai sričiai yra skiriamas pakankamas dėmesys.



16 pav. **Reguliarus įrangos ir priemonių, skirtų apsisaugoti nuo grėsmių, atnaujinimas**

Teigti, kad organizacija yra pasiruošusi įvairioms grėsmėms galima tada, jei ji turi planą, padėsianti numatyti galimas rizikas, įvertinti jų poveikį ir imtis veiksmų užtikrinančių IT organizacijos veiklos tęstinumą.

Apklausos duomenimis respondentų nuomonė šiuo klausimų išsiskyrė, didžioji dalis atsakiusiųjų, t.y. 83 proc. nežinojo ar organizacija turi bent vieną iš minimų planų (17 pav.).



17 pav. **Pasiruošimo ekstremaliosioms situacijoms planas**

Tokie pat rezultatai buvo gauti atliekant pirminę apklausą kur nuomonė šiuo klausimu pasiskirstė į tris dalis. Vieni teigė, kad nieko nežino apie tokio plano buvimą, kiti tvirtino, kad plano nėra, o treti – teigė, kad planas yra. Pasitaikė respondentų, kurie atsakė, kad organizacija turi tęstinės veiklos planą (11 proc.) ar parengties ekstremaliosioms situacijoms planą (2 proc.). Tačiau atsižvelgiant į žvalgybinio tyrimo rezultatus, kur buvo įvardinta, kad yra „tinklo apsaugos sistemos, ribojamas patekimas į patalpas“ (I3-1), „apsaugotas vidinis tinklas, ugniasienė, patalpų apsauga, (...)“ (B3-2), darytinos išvados, kad respondentų atsakymą suklaidino taikoma įprastinė apsauga, kurią jie palaikė pateiktais planais. Taip pat buvo klausiama kokios priežastys lėmė, kad tokio plano organizacija neturi. Be to, siekiant pasitikslinti, ar toks planas vis dėlto yra, buvo paklausta organizacijos vadovų ir buvo gautas neigiamas atsakymas (4 lent.).

4 lentelė. Organizacijos apsaugos nuo grėsmių planas

Respondentų pasisakymai	Potemė	Tema
Nežinau (A3-2)	Informacijos stoka	Informacijos dėl plano buvimo stoka
Nežinau (C3-3)		
Nežinau (D3-4)		
Nežinau (E3-2)		
Nežinau (F3-2)		
Nežinau (G3-2)		
Nežinau (J3-2)		
Taip. Apsaugotas vidinis tinklas, ugniasienė, patalpų apsauga, ribojamas patekimas į patalpas (B3-2)	Yra planas	Plano įvardijimas
Taip. Tinklo apsaugos sistemos, ribojamas patekimas į patalpas (I3-1)		

4 lentelės tęsinys kitame puslapyje

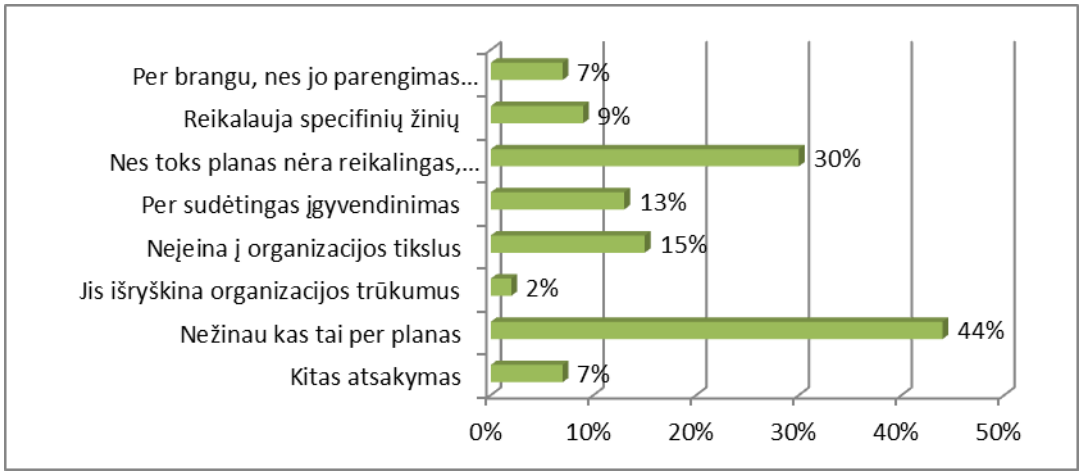
4 lentelės tęsinys

Respondentų pasisakymai	Potemė	Tema
Ne, nes nebuvo precedento (H3-2)	Plano poreikio neįžvelgimas	Plano nebuvimo priežastys
Rašytinio plano nėra, tiesiog stiprinamos grėsmingos vietos (K3.1-2)	Susitelkimas į tam tikras sritis	
Tikimybės ir rizikos faktorius nepakankamas. Be to, kas liečia infrastruktūros kiek žinau toks planas atsiras (K3.2-3)	Grėsmių ir pasekmių neįžvelgimas	
Neturi, nes neįžvelgiamos grėsmės ir pasekmės (L3.2-3)		

4 proc. respondentai teigė, kad organizacija neturi nei vieno iš aukščiau nurodytų planų. Tie, kurie pasakė, kad plano nėra, pabrėžė, kad „rašytinio plano nėra, tiesiog stiprinamos grėsmingos vietos“ (K3.1-2). O toks planas neatsirado, kadangi, pasak apklaustojo (H3-2), „nebuvo precedento“. Manytina, kad nederėtų laikytis tokios pozicijos, kadangi tokie planai turėtų būti rengiami kol ekstremalioji situacija dar nepasireiškė ir organizacija nepaliesta grėsmių, nes jai įvykus reikės pradėti veikti, o ne dalinti pareigas ir svarstyti kas už kokius veiksmus galėtų būti atsakingas. Remiantis sekančia nuomone, plano nėra, nes „neįžvelgiamos grėsmės ir pasekmės“ (L3.2-3). Tai parodo, kad nėra suvokiama kokį poveikį gali padaryti įvykusi ekstremalioji situacija. Kitas respondentas paaiškino, kad plano nėra, kadangi „tikimybės ir rizikos faktorius nepakankamas. Be to, kas liečia infrastruktūros kiek žinau toks planas atsiras“ (K3.2-3). Vertinant tiriamojo pasisakymą, darytinos išvados, kad kol kas grėsmės nepasiekė tokio lygio, jog reikėtų sudaryti planus skirtus apibrėžti organizacijos veiksmus ekstremaliųjų situacijų atveju.

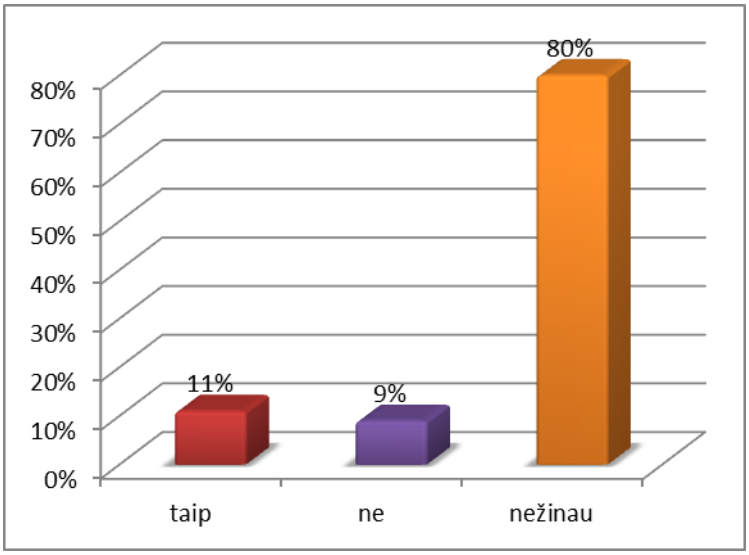
Plačiau nagrinėjant priežastis (18 pav.), sąlygojančias tokio plano nebuvimą 44 proc. respondentų teigė, jog nežino, kas tai per planas. O 30 proc. kaip vieną iš priežasčių, kodėl jų manymu, organizacija neturi tęstinės veiklos plano įvardijo tai, jog toks planas nėra reikalingas, nes yra mažai tikėtina, kad aukščiau išvardintos rizikos paveiks organizacijos veiklą. Šis teiginys sutampa su aukščiau išsakytu respondento (L3.2-3) teiginiu, kad nėra įžvelgiamos grėsmės ir pasekmės. Tai dar kartą patvirtina, kad respondentai nesuvokia galimos rizikos. Šią prielaidą taip pat patvirtina respondento išsakytas teiginys: „Manau, darbuotojai netraktuotų to kaip itin svarbaus dokumento, todėl net ir tokį turint neteiktų jam daug dėmesio“ (R3). Tarp atsakančiųjų pasitaikė tokių, kurie negalėjo įvardinti plano neturėjimo priežasčių, nes pasakė, kad „nežinau ar toks planas yra, todėl negaliu atsakyti į šį klausimą“ (R24). Arba teigė neprisimenantys apie tokio plano egzistavimą: „Nepamenu, ar bendrovė turi šiuos dokumentus (spėju, kad turi)“ (R6). Pirmas veiksnys įrodantis, kad organizacijoje nėra kuriama saugumo kultūra yra tai, jog darbuotojai neturi aiškios informacijos susijusios su pasiruošimo ekstremaliosioms situacijoms planu.

Šiuo atveju antra hipotezė pasitvirtino, o tai reiškia, kad tiriama organizacija neturi plano aprašančio pasiruošimo veiksmus ekstremaliosioms situacijoms.



18 pav. **Plano skirto ekstremaliosioms situacijoms stokos priežastys**

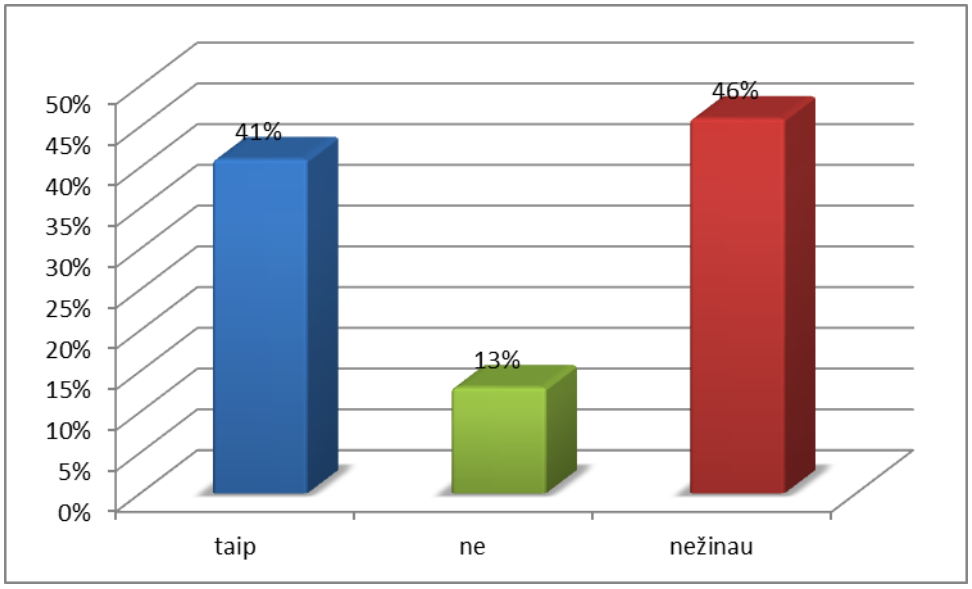
Kadangi organizacijoje nėra tęstinės veiklos plano, todėl buvo siekiama išsiaiškinti, ar yra koks kitas planas, kuris ekstremaliosios situacijos atveju palengvintų organizacijos grįžimą prie įprastinės veiklos. Deja, ir šiuo atveju buvo susidurta su panašia situacija, nes 80 proc. iš dalyvavusių apklausoje pasakė, kad nežino ar yra kitas planas (19 pav.).



19 pav. **Kitas planas, palengvinantis grįžimą prie įprastinės veiklos**

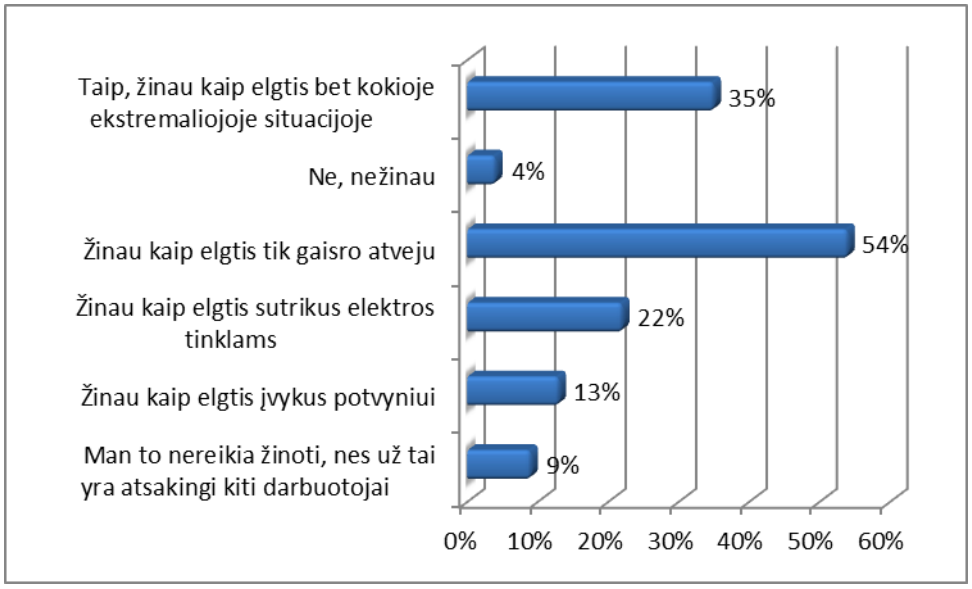
Jeigu darbuotojų nuomonė pateiktais klausimais skiriasi, vadinasi, jie nėra informuoti apie tokių planų buvimą. Tada kyla klausimas ar yra organizacijoje asmenys atsakingi už civilinę saugą. Atsakymai tarp taip (41 proc.) ir nežinau (46 proc.) pasiskirstė su 5 proc. skirtumu. O vertinant didelį

skirtumą tarp taip ir ne atsakymų pastebima, kad respondentų teigimu organizacija turi asmenį arba skyrių, kuris yra atsakingas už organizacijos apsaugos priemones nuo grėsmių (20 pav.).



20 pav. **Už civilinę saugą atsakingo žmogaus buvimas**

Remiantis atlikta tyrimo analize aiškėja, kad įvykus ekstremaliajai situacijai organizacija neturi plano padėsiančio jai atsigauti ir toliau tęsti savo veiklą. Atsižvelgiant į tai, bandoma išsiaiškinti, ar susidūrus su grėsmėmis esant darbo vietoje, darbuotojai žinotų ką, kokiomis situacijomis reikėtų daryti (21 pav.).



21 pav. **Žinojimas kaip elgtis ekstremaliosios situacijos atveju esant darbo vietoje**

Daugiausia (54 proc.) pasirinktų atsakymų liudijo, jog respondentai žino kaip elgtis gaisro atveju, o taip pat teigė, jog žino kaip elgtis bet kokioje ekstremaliojoje situacijoje. Tarp labiausiai

pasirenkamų (22 proc.) atsakymų variantų buvo ir žinojimas kaip elgtis sutrikus elektros tinklams. Tai ypač svarbu dirbant su priemonėmis, kurios sudaro darbo pagrindą. Taip pat buvo manančių, jog jiems nereikia žinoti kaip elgtis susidarius ekstremaliajai situacijai, kadangi tą turi žinoti už tai atsakingi asmenys. Kaip ir analizuojant organizacijos pasiruošimą įveikti grėsmes taip ir šiuo atveju buvo įvardinta kitų asmenų atsakomybė už veiksmus ekstremaliosiose situacijose.

Nepaisant to, kad respondentai nurodė, jog žinotų, ką reikėtų daryti tam tikromis situacijomis vis dėlto darytinos prielaidos, kad to žinojimo šaltiniai yra skirtingi. Kaip nurodė apklaustieji jie žinotų kaip elgtis ekstremaliųjų situacijų metu ir tai jiems yra žinoma „iš darbo saugos dokumento“ (I4-3) arba „iš saugumo technikos taisyklių“ (C4-5). Kiti paminėjo, kad tokie dalykai jiems yra savaime suprantami (B4-4) ir žino tą „iš bendro išprusimo“ (E4-4). Tačiau nei vienas iš respondentų nenurodė, kad jų žinios yra lydimos specialaus tam skirto plano ar veiklos tęstinumo užtikrinimo plano. Nurodymų kaip elgtis ekstremaliosios situacijos atveju stoka yra kitas reikalavimas reikalingas saugumo kultūrai patvirtinti, kuris, deja, taip pat nėra įvykdytas.

Jeigu, kaip nurodė respondentai organizacija yra pažeidžiama, o dokumento, kuriuo būtų galima vadovautis nėra, tada yra svarstoma ar patys darbuotojai imasi kokių nors apsisaugojimo priemonių ar ne, jei taip tai dėl kokių priežasčių jie tai daro (5 lent.).

5 lentelė. Savarankiško apsisaugojimo priežastys

Respondentų pasisakymai	Potemė	Tema
Atsakomybė įmonei, kurioje dirbu (A5-5)	Atsakomybė	Priežastys skatinančios savarankišką saugojimąsi nuo grėsmių
Noras apsisaugoti nuo galimos žalos (E5-5)		
Noras apsaugoti save ir kolegas nuo nelaimės (F5-5)		
Žmogiškasis faktorius (C5-6)		
Sveikas protas (H5-5)		
Noras apsaugoti įmonę nuo potencialių nuostolių (F5-6)		
Duomenų svarbumas (B5-5)	Baimė prarasti duomenis	
Organizacijos duomenų svarba (I5-4)		

5 lentelės tęsinys kitame puslapyje

5 lentelės tęsinys

Respondentų pasisakymai	Potemė	Tema
Taip. Baimė prarasti, sugadinti turimą informaciją, duomenis, įmonės turtą ir t.t. (j5-4)	Baimė prarasti duomenis	Priežastys skatinančios savarankišką saugojimąsi nuo grėsmių
Suinteresuotumas nekenkti organizacijai, kurioje dirbu (D5-8)	Ištikimybė organizacijai	
Lojalumas (A5-4)		
Geras būdas (D5-7)	Asmeninės savybės	
Patirtis (G5-4)	Patirtis	
Taip. Stipriname kompetencijas (k5-5)	Sistemų tobulinimas	Veiksmai patvirtinantys savarankišką saugojimąsi
Optimizuojame procesus (K5-6)		
Taip, laikausi standartinių saugumo normų (L5-6)	Vadovavimasis saugumo taisyklėmis	

Bandant sužinoti ar respondentai yra linkę savarankiškai imtis saugumo priemonių įvykus ekstremaliajai situacijai, nors ir negauna nurodymų, ir nesivadovauja planu, buvo klausiama ar jie imasi saugumo priemonių savarankiškai ir kas juos skatina taip elgtis.

Nepaisant to, kad nėra nustatyta įpareigojančių taisyklių kaip elgtis tokių situacijų metu, visi respondentai nurodė, kad savarankiškai imasi reikalingų saugumo priemonių. Taip elgtis juos skatina atsakomybė prieš įmonę, kadangi norima „apsaugoti ją nuo potencialių nuostolių“ (F5-6), o, be to, siekiama „apsaugoti save ir kolegas nuo nelaimės“ (F5-5), taip pat „(...) nuo galimos žalos“ (E5-5). Darbuotojai suvokia, kad darbas technologijų srityje reikalauja ypatingo atsargumo bei budrumo (H5-5).

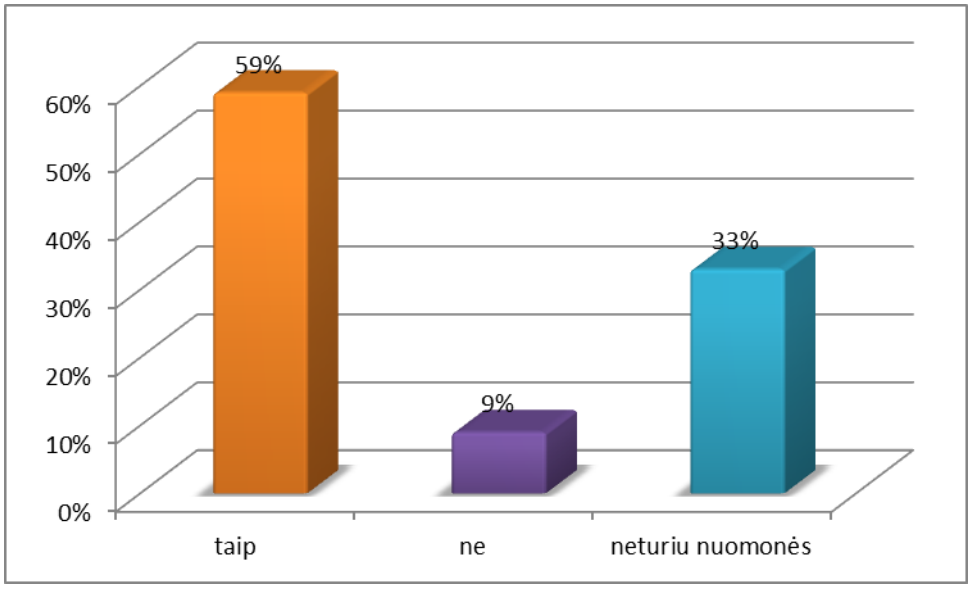
Baimė prarasti duomenis (I5-4; J5-4) taip pat yra įvardijama kaip viena iš priežasčių, skatinanti savarankišką apsisaugojimą nuo grėsmių. Bijoma prarasti ne tik sukauptą informaciją, duomenis, kas reiškia, kad tai yra darbo rezultatai (I5-4; J5-4), bet ir įmonės turtą. Taigi baimė dėl duomenų yra viena iš varomųjų jėgų savarankiško saugumo srityje.

Ištikimi darbuotojai yra vienas iš saugumo garantų, nes lojalūs (A5-4; D5-8) darbuotojai yra atsakingi darbuotojai.

Bandymus savarankiškai imtis saugumo priemonių galima vertinti kaip suvokimą, kad ekstremalioji situacija gali įvykti. Tačiau išvardintos priežastys leidžia tuo abejoti, kadangi atsakomybė ir ištikimybė organizacijai nepatvirtina to, kad yra suvokiama galima žala. Viena iš svaresnių priežasčių yra baimė prarasti turimus duomenis, nes tai gali pakenkti organizacijos veiklai. Todėl nepaisant darbuotojų ištikimybės ir atsakingumo vis dėlto patartina apsidrausti ir turėti planą, su kuriuo būtų supažindinti visi darbuotojai. Nepaisant to, kad darbuotojai patys imasi apsaugos

priemonių nuo grėsmių vis dėlto kaip buvo minėta anksčiau (žr. 1 sk.), savarankiški saugumo veiksmai bus trumpalaikiai, jei organizacija nepuoselės saugumo kultūros ir neturės aiškaus veiksmų plano.

Tačiau siekiant geriau suprasti kaip darbuotojai suvokia rizikas, buvo klausiama ar jų manymu, reikia organizacijai dokumento, kuris padėtų pasiruošti ekstremaliajai situacijai ir veikti po jos. Nepaisant to, kad respondentai neturėjo informacijos apie tokio plano buvimą, vis dėlto daugiau nei pusė dalyvavusių apklausoje įžvelgė tokio plano poreikį, už tai pasisakė 59 proc. Šiuo klausimu nuomonės neturėjo 33 proc. (22 pav.)



22 pav. **Dokumento, reglamentuojančio ekstremaliosios situacijos veiksmus, poreikis**

Nors respondentai neturėjo informacijos apie kito plano, palengvinančio organizacijos grįžimą prie įprastinės veiklos, buvimą, vis dėlto jie įžvelgė tokio plano poreikį. Jam atsirasti ateityje yra nurodoma nemažai priežasčių bei tokio plano privalumų (žr. 6 lent.).

6 lentelė. Priežastys lemiančios plano atsiradimą

Respondentų pasisakymai	Potemė	Tema
Žinoma. Jeigu tokio nebūtų – padidėtų grėsmių tikėtinumas (b3.2.1.-3)	Apsauga nuo grėsmių	Priežastys skatinančios plano atsiradimą
Toks planas yra gerai, kad apsisaugoti nuo grėsmių (C3.2.1.-4)		
Taip, kadangi be jo stipriai išaugtų grėsmių tikimybė (I3.2.1.-2)		
Taip, protinga yra saugoti ir rūpintis savo resursais (D3.2.1.-5)	Saugoti išteklius	

6 lentelės tęsinys kitame puslapyje

6 lentelės tęsinys

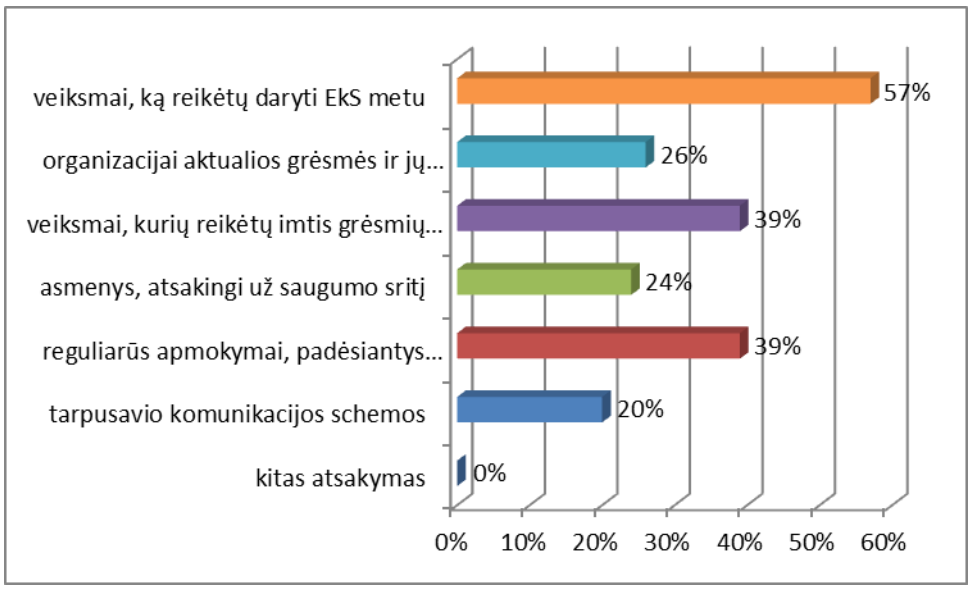
Respondentų pasisakymai	Potemė	Tema
Taip, nes užtikrina veiklos tęstinumą (F3.2.1-3)	Tolimesnės veiklos užtikrinimas ir stiprinimas	Priežastys skatinančios plano atsiradimą
Reikalingas, nes jis padės geriau valdyti kritines vietas (K3.2.1.-2)		
Taip. Įvykus minėtoms grėsmėms turi būti atsakingas asmuo, kuris žinotų kaip elgtis tokioje situacijoje (h3.2.1.-3)	Už ekstremaliąsias situacijas atsakingas specialistas	
Galbūt būtų neblogai, tačiau jis, mano nuomone, nėra būtinas (E3.2.1.-3)	Nėra būtinybės	Neįžvelgiamas plano poreikis
Ne (J3.2.1.-3)		

Respondentų manymu, esant planui sumažėtų galimų grėsmių tikimybė (B3.2.1-3; I3.2.1.-2), kadangi būtų galimybė nuo jų apsisaugoti. Turima gera apsauga prisidėtų prie turimų organizacijos išteklių tausojimo (D3.2.1.-5). Be to, tokio plano būtinybė yra įžvelgiama dėl poreikio toliau tęsti ir stiprinti vykdomą veiklą (F3.2.1-3; K-2). Tą patvirtina organizacijos darbuotojo teiginys, kad „(...) jis padės geriau valdyti kritines vietas“ (K3.2.1-2).

Kadangi tokio plano privalumų ir priežasčių jam atsirasti yra įžvelgiama nemažai, todėl darytinos prielaidos, kad organizacijai toks planas yra reikalingas. Vis dėlto tarp apklaustųjų atsirado tokių, kurių nuomone, pasiruošimo ekstremaliosioms situacijoms planas nėra reikalingas (E3.2.1.-3; J3.2.1-3) (žr. 22 pav.) Tačiau rezultatai patvirtina, kad respondentai nėra bendrai informuoti ką privalėtų daryti susiklosčius ekstremaliajai situacijai, todėl plano būtinybė yra įžvelgiama.

Iškelta trečia hipotezė, kuri teigė, kad respondentai neįžvelgia tęstinės veiklos plano poreikio savo organizacijai, nepasitvirtino. Remiantis apklausos rezultatais šiek tiek daugiau negu pusė apklaustųjų, t.y. 27 respondentai (59 proc.) pasisakė už tokio plano poreikį.

Kadangi dauguma respondentų pasisakė už tai, kad tokio dokumento reikėtų, todėl jų klausiama, kokia jų nuomone, informacija galėtų būti jame nurodyta (23 pav.).



23 pav. **Informacija pateikta dokumente, reglamentuojančiame ekstremaliųjų situacijų veiksmus**

Tarp daugiausiai pasirenkamų atsakymų buvo nurodyti veiksmai, kurie apibrėžtų, ką reikėtų daryti įvykus ekstremaliajai situacijai (57 proc.). Respondentų balsai pasiskirstė po lygiai, t.y. po 39 proc. atsakymų buvo skirta veiksmams, kurių reikėtų imtis grėsmių poveikiui sumažinti ir reguliariems apmokymams, padėsiantiems nepasimesti ekstremaliojoje situacijoje. Atsižvelgiant į tokį pasirinkimą, darytinos prielaidos, kad organizacijai tinkamiausias yra veiklos tęstinumo užtikrinimo planas. Taip pat svarbiomis laikytinomis organizacijai aktualios grėsmės ir jų tikimybės.

Remiantis rezultatais darytinos išvados, kad darbuotojai norėtų, kad būtų toks planas, kuris reglamentuotų jų veiksmus ekstremaliosiose situacijose ir, kuriuo remiantis darbuotojai būtų apmokomi elgtis tokiose situacijose.

3.3. Tyrimo išvados

1. Tyrimas atskleidė, kad organizacija neturi plano, kurio dėka būtų pasiruošta ekstremaliosioms situacijoms. Tokio plano stoką nulėmė netinkamas grėsmių suvokimas, t.y. manoma, kad yra maža tikimybė, kad pasireiškusios grėsmės galėtų turėti poveikį organizacijai. Tai parodo, kad nėra įvertintas šių grėsmių galimas poveikis organizacijos veiklai, o taip pat vyrauja informacijos trūkumas dėl plano paskirties.
2. Pripažįstama, kad dėl vykdomos veiklos pobūdžio bei santykinių apsaugų priemonių taikymo, kurios yra pritaikytos tik tam tikroms grėsmėms, organizacija yra pažeidžiama. Nors organizacijoje labiau yra įžvelgiamos technologinės grėsmės, kurios yra tiesiogiai susijusios su jos veikla, vis dėlto jai nederėtų ignoruoti kitokio pobūdžio grėsmių, kurios taip pat gali paveikti organizacijos veiklą.

3. Nepaisant to, kad organizacija atnaujina apsisaugojimo resursus, vis dėlto į vykdomus mokymus nėra įtraukti visi darbuotojai, taip pat ne visi žino ar yra vykdoma rizikų analizė, o stiprinant apsaugos priemones yra orientuojamasi tik į tam tikras grėsmes. Dėl šių priežasčių įvardinto pasiruošimo ekstremaliosioms situacijoms negalima laikyti pagrįstu.
4. Nors žvelgiant į dabartinę situaciją organizacija neturi plano, vis dėlto įžvelgiamas dokumento, reglamentuojančio organizacijos veiksmus ekstremaliųjų situacijų metu, poreikis ateityje. Organizacijos darbuotojai supranta, jog jis ne tik palengvintų apsaugą nuo grėsmių, bet ir leistų užtikrinti veiklos tęstinumą.
5. Žvelgiant į susiklosčiusią situaciją, darytina išvada, kad dėl rizikų nesuvokimo organizacija nesiruošia ekstremaliosioms situacijoms, tačiau norėtų tokių veiksmų imtis ateityje.
6. Dėl dokumento stokos, darbuotojai baimindamiesi prarasti turimus darbo rezultatus, sukauptą informaciją, pradeda savarankiškai taikyti apsaugos priemones, kurios nėra apibrėžtos vienu bendru dokumentu. Deja, toks apsisaugojimas gali būti neveiksmingas, nes bus trumpalaikis.
7. Atliktu tyrimu buvo patvirtintos iškeltos dvi hipotezės, kad technologinės grėsmės yra įžvelgiamos kaip didžiausią poveikį IT organizacijos veiklai turinčios ir, kad organizacija neturi plano skirto pasiruošti ekstremaliosioms situacijoms. Viena iškelta hipotezė, kad darbuotojai neįžvelgia tęstinės veiklos plano reikalingumo, buvo paneigta.

IŠVADOS IR REKOMENDACIJOS

1. Rizikos suvokimas yra subjektyvus veiksnys, formuojantis individo požiūrį į jam kylančias grėsmes. Vyraujantis suvokimas gali būti pagrįstas tiek turima patirtimi, tiek informacijos apimtimi, asmeninėmis nuostatomis, žiniomis, įsivaizdavimais ir daugeliu kitų faktorių. Rizikos suvokimo aiškinimas gali skirtis priklausomai nuo psichologinio, politinio, kultūrinio ir socialinio požiūrių. Norint priimti teisingus sprendimus ekstremaliųjų situacijų metu, žinoti savo pareigas bei atsakomybę, o taip pat patirti mažiau įtampos galima imtis pasiruošimo veiksmų. Imantis pasiruošimo veiksmų svarbu įvertinti vyraujanti suvokimą, nuo kurio priklauso gresiančios situacijos įvertinimas ir reagavimas.
2. Organizacijos pasiruošimas ekstremaliosioms situacijoms priklauso nuo individų rizikos suvokimo. Esant suvokimui, jog yra rizika grėsmei pasireikšti yra imamasi priemonių, padėsiančių apsisaugoti nuo ekstremaliosios situacijos ir formuoti rizikos suvokimą. Organizacijoje vertinančioje save kaip pažeidžiamą vyraus aukštas rizikos suvokimas, todėl ji sieks pasiruošti įvykiui. Suvokusi tokio pasiruošimo svarbą organizacija paruoš planus, rengs mokymus darbuotojams, kurių metu bus patikrinami ne tik esami gebėjimai, bet ir suteikiamos naujos kompetencijos kaip elgtis ekstremaliosiose situacijose, o rašytinių planų veiksmingumą patikrins pratybų metu.
3. Tyrimas, atliktas IT organizacijoje, atskleidė, kad organizacija nėra pasiruošusi galimoms ekstremaliosioms situacijoms. Šios išvados yra daromos atsižvelgiant į išskirtas, organizacijos grėsmes bei plano, skirto pasiruošti ekstremaliosioms situacijoms trūkumą. Susiklosčiusi padėtis kelia rūpestį, kadangi susidarius tokiai situacijai, yra tikėtina, kad organizacija nesugebės tinkamai reaguoti bei toliau tęsti savo veiklos.
4. Tik savo darbo srities, t.y. technologinių grėsmių, įžvelgimas sąlygoja ribotą apsisaugojimą, kuris negali apsaugoti nuo visų grėsmių ir būti tinkamas nenumatytoms situacijoms. Būtent todėl organizacijos pažeidžiamumas didėja, o darbuotojų įtraukimo tiek į mokymų procesą, tiek į atliekamą rizikų analizę trūkumas skatina pačius darbuotojus rūpintis apsaugos priemonėmis, kurios gali būti netinkamos.
5. Organizacijos darbuotojai yra atviri pokyčiams, nes supratę, kad negali išvengti grėsmių, norėtų turėti dokumentą, kuriame būtų apibrėžti veiksmai kurių reikėtų imtis ekstremaliųjų situacijų metu ir galimų grėsmių poveikio sumažinimo priemonės.

Atsižvelgiant į pateiktas išvadas, organizacijoms siekiančioms sukurti pasiruošimo ekstremaliosioms situacijoms priemones bei ketinančioms užtikrinti savo veiklos tęstinumą po ekstremaliosios situacijos **rekomenduotina:**

1. Parengti tęstinės veiklos planą, kuris ne tik padėtų imtis prevencinių priemonių, pasiruošti, bet ir būtų orientuotas į veiksmus po ekstremaliosios situacijos, t.y. į organizacijos atsigavimą ir veiklą po susidariusios situacijos.
2. Plane turėtų būti numatytas plano tikslas, apibrėžtos darbuotojų pareigos ir jų atsakomybės už tam tikrus veiksmus, pasireiškus ekstremaliajai situacijai. Į planą turėtų būti įtraukta rizikų analizė, t.y. reikėtų įvertinti kokios yra galimos rizikos, kokia jų pasireiškimo tikimybė ir kaip bei kokias pažeidžiamas sritis jos galėtų paveikti. Apsibrėžus grėsmes, patartina numatyti apsaugos nuo jų priemones.
3. Taip pat patartina sudaryti mokymų programą, kurioje būtų pateiktos įvairios situacijos priklausomai nuo pasireiškiančių grėsmių ir tų situacijų valdymo būdai. Mokymų metu būtų patikrinamas plano praktinis įgyvendinimas.
4. Į pasiruošimo plano rengimo procesą siūloma įtraukti kiek galima daugiau darbuotojų. Šis veiksmas padėtų išsiaiškinti, kaip darbuotojai suvokia galimas rizikas, kaip jie vertina galimas grėsmes. Tokiu būdu būtų išplečiamas suvokiamų rizikų ratas, o tai padėtų išsamiau sudaryti pasiruošimo ekstremaliosioms situacijoms planą.
5. Remiantis sudarytu pasiruošimo planu vykdyti mokymus, kuriuose atsispindėtų plane nurodyti veiksmai, kurie suteiktų žinių veikti ekstremaliosiose situacijose. O vykdant pratybas, patikrinti plano veiksmingumą, analizuoti bei pašalinti esančius trūkumus.

LITERATŪRA

1. **Al - Badi A. H. ir kt.** IT disaster recovery: Oman and Cyclone Gonu lessons learned // Information management and computer security, 2009, vol. 17, no. 2, p. 114 – 126.
2. **Balžekienė A.** Rizikos suvokimas: sociologinė konceptualizacija ir visuomenės nuomonės tyrimo metodologinės prielaidos // Filosofija. Sociologija. – Kaunas: Lietuvos mokslų akademija Lietuvos mokslų akademijos leidykla, 2009, T. 20, Nr. 4, p. 217 – 226. http://archive.minfolit.lt/arch/21501/21927.pdf [žiūrėta 2012 09 30]
3. **Berg B. L.** Qualitative research methods for the social sciences / 6th ed. – Boston (Mass): Pearson: Allyn and Bacon, 2007. – 384 p.
4. **Bitinas B. ir kt.** Kokybinių tyrimų metodologija: vadovėlis vadybos ir administravimo studentams. – Klaipėda: S. Jokužio leidykla – spaustuvė, 2008. – 303 p.
5. **Bye R., Lamvik G. M.** Organizational culture and risk perception // Zagadnienia eksploatacji maszyn, 2007, vol. 42, nr. 2, p. 131- 146. http://t.tribologia.eu/plik/spm/spmom-07v42n2_p-131.pdf [žiūrėta 2013 02 21]
6. **Blades A.** Business continuity planning: protecting your organization‘s life / edited by Ken Doughty. – Boca Raton (Fla.); London; New York (N.Y.); Washington: CRC Press Press: Taylor and Francis, 2001. http://web.ebscohost.com.skaitykla.mruni.eu/ehost/ebookviewer/ebook/ZTAwMHh3d19fMTM1NDgyX19BTg2?sid=f8e1a2bd-cad6-4599-ae6a-0352d9eef71c@sessionmgr10&vid=3&format=EB&rid=8 [žiūrėta 2013 09 25]
7. **Blyth M.** Risk and security management: protecting people and sites worldwide. – Hoboken (N. J.): John Wiley, 2008. – 401 p.
8. **Boyne R.** Risk. – Buckingham; Philadelphia (Pa.): Open University Press, 2003. – 132 p.
9. **Borodzicz E. P.** Risk, crisis and security management. – Chichester; Hoboken (N. J.): John Wiley, 2005. – 244 p.
10. **CDEM exercises: Directors guidelines for Civil Defence Emergency Management**, 2009. http://www.civildefence.govt.nz/memwebsite.nsf/Files/Director_Guidelines/$file/CDEM_exercises_web.pdf [žiūrėta 2013 04 10]
11. **Cerullo V., Cerullo M. J.** Business continuity planning: a comprehensive approach // Information Systems Management, 2004, vol. 21, no. 3, p. 70 – 78. http://www.tandfonline.com.skaitykla.mruni.eu/doi/pdf/10.1201/1078/44432.21.3.20040601/82480.11 [žiūrėta 2013 04 10]

12. **Crouhy M. ir kt.** The Essentials of risk management. – New York (N.Y.): McGraw-Hill, 2006. – 414 p.
13. **Davidson Frame J.** Managing risk in organizations: a guide for managers. – San Francisco: Jossey Bass, 2003. – 264 p.
14. **Denney D.** Risk and society. – London; Thousand Oaks (Calif.); New Delhi: Sage Publications, 2005. – 220 p.
15. **Didžiulienė R.** Sociologija: mokomoji knyga. – Kaunas: Technologija, 2004. – 60 p.
16. **Draper E.** Risk, society, and social theory // Contemporary Sociology, 1993, vol. 22, no. 5, 641 – 644 p. http://www.jstor.org.skaitykla.mruni.eu/stable/pdfplus/2074588.pdf?acceptTC=true&acceptTC=true&jpdConfirm=true [žiūrėta 2012 10 29]
17. **Duncan W. J. ir kt.** Surviving organizational disasters // Business horizons, 2011, vol. 54, issue 2, p. 135 – 142. http://www.sciencedirect.com.skaitykla.mruni.eu/science/article/pii/S0007681310001515 [žiūrėta 2012 10 25]
18. **Fischhoff B.** Risk perception and communication unplugged: twenty years of process // Risk Analysis, 1995, vol. 15, no. 2, 137 – 145 p.
19. **Garcia del Castillo J. A.** Concepto de percepcion de riesgo y su repercusion en las adicciones // Salud y Drogas, 2012, vol. 12, no. 2, 133 – 151 p. http://www.redalyc.org/pdf/839/83924965001.pdf [žiūrėta 2013 05 27**]**
20. **Guščinskienė J.** Taikomoji sociologija. – Kaunas: Technologija, 2004. – 94 p.
21. **Hopkin P.** Fundamentals of risk management: understanding, evaluating, and implementing effective risk management. - London; Philadelphia (Pa): New Delhi: Kogan Page, 2010. – 357 p.
22. **Hopkins A.** What are we to make safe of behaviour programs? // Safety science, vol. 44, issue 7, 2006, 583 – 597 p. http://ac.els-cdn.com.skaitykla.mruni.eu/S0925753506000026/1-s2.0-S0925753506000026-main.pdf?_tid=f36f843c-43c7-11e3-8eb8-00000aab0f6c&acdnat=1383401361_3b3418d4b31ddcc65fc9787d9c5d73cd [žiūrėta 2013 03 19]
23. **Hudson P.** Safety culture – theory and practice // RTO MP - 032, 1999, p. 2 – 12. http://ftp.rta.nato.int/public//PubFulltext/RTO/MP/RTO-MP-032///MP-032-08.pdf [žiūrėta 2013 02 21]
24. **Jackson B. A. ir kt.** Are we prepared? Using reliability analysis to evaluate emergency response systems // Journal of Contingencies and Crisis Management, 2011, vol. 13, issue 3, p.

147 – 157 p. http://onlinelibrary.wiley.com/doi/10.1111/j.1468-5973.2011.00641.x/pdf [žiūrėta 2013 03 05]

25. **Janušonis V.** Rizikos valdymas sveikatos priežiūros organizacijose: monografija. – Klaipėda: S. Jokužio leidykla – spaustuvė, 2005. – 253 p.
26. **Kardelis K.** Mokslinių tyrimų metodologija ir metodai: edukologija ir kiti socialiniai mokslai: vadovėlis / 3-iasis leidimas. – Šiauliai: Lietuvos kūno kultūros akademija, 2005. – 398 p.
27. **Kildow B. A.** A supply chain management guide to business continuity / 1st ed. – New York: American management association, 2011. – 289 p. http://web.ebscohost.com.skaitykla.mruni.eu/ehost/ebookviewer/ebook/e000xww_352621_AN?sid=17086215-c558-405c-b2a5-7d2633072bd6@sessionmgr14&vid=3&format=EB&rid=1 [žiūrėta 2013 10 20]
28. **Lindell M. K. ir kt.** Fundamentals of emergency management. – Emmitsburg, MD: Federal emergency management agency emergency management institute, 2006. – 479 p. http://www.training.fema.gov/EMIWeb/edu/fem.asp [žiūrėta 2013 02 04]
29. **Lovekamp W. E., Tate M. L.** College student disaster risk, fear and preparedness // International Journal of Mass Emergencies and Disasters, 2008, vol. 26, no. 2, p. 70 – 90. http://ijmed.org/articles/285/download/ [žiūrėta 2012 10 25]
30. **Luobikienė I.** Sociologinių tyrimų metodika: mokomoji knyga. – Kaunas: Technologija, 2006. – 121 p.
31. **Lupton D.** Risk / 2nd ed. – Routledge: Taylor and Francis Group, 1999a. – 266 p. http://books.google.lt/books?id=_y8hE6O2dbMC&printsec=frontcover&hl=lt&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [žiūrėta 2013 01 22]
32. **Lupton D., Tulloch J.** Risk is part of your life: risk epistemologies among a group of Australians // Sociology, 2002, vol. 36 (2), p. 317 – 334. http://soc.sagepub.com.skaitykla.mruni.eu/content/36/2/317.full.pdf+html [žiūrėta 2013 01 13]
33. **McEntire D. A., Myers A.** Preparing communities for disasters: issues and processes for government readiness // Disaster Prevention and Management, 2004, vol. 13, no. 2, 140 – 152 p.
34. **Merna T., Al – Thani F.** Corporate risk management / 2nd ed. – Chichester: John Wiley, 2008. – 422 p.

    Mileti D. S. Disasters by design: a reassessment of natural hazards in the United States. – Washington: Joseph Henry Press, 1999. – 351 p. http://books.google.lt/books?id=bkNPlhhK1fgC&printsec=frontcover&hl=lt&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [žiūrėta 2013 02 01]

35. **Mitroff I. I. ir kt.** Effective crisis management // The Academy of Management Executive, 1987, vol. 1, no. 3, p. 283 – 292. http://www.paulshrivastava.net/Research%20Publications%20Directory%5Ceffective%20crisis%20managment.pdf [žiūrėta 2013 02 23]
36. **Mitroff I. I. ir kt.** The structure of man-made organizational crises: conceptual and empirical issues in the development of a general theory of crisis management / Key readings in crisis management: systems and structures for prevention and recovery / Denis Smith, Dominic Elliott, editors. – London; New York (N.Y.): Routledge: Taylor and Francis Group, 2006. – 436 p.
37. **Paton D.** Disaster preparedness: a social – cognitive perspective // Disaster Prevention and Management, 2003, vol. 12, no. 3, p. 210 – 216.
38. **Paton D. ir kt.** Volcanic hazards: risk perception and preparedness // New Zealand Journal of Psychology, 2000, vol. 29, no. 2. http://www.psychology.org.nz/cms_show_download.php?id=701 [žiūrėta 2013 01 13]
39. **Paton D., Flin R.** Disaster stress: an emergency management perspective // Disaster Prevention and Management, 1999, vol. 8, no. 4, p. 261-267.
40. **Paton D., Johnston D.** Disasters and communities: vulnerability, resilience and preparedness // Disaster Prevention and Management, 2001, vol. 10, no. 4, p. 270 – 277.
41. **Perry R. W.** Disaster exercise outcomes for professional emergency personnel and citizen volunteers // Journal of Contingencies and Crisis Management, 2004, vol. 12, no. 2, 64 – 75 p. http://onlinelibrary.wiley.com/doi/10.1111/j.0966-0879.2004.00436.x/pdf [žiūrėta 2013 01 27]
42. **Perry R. W., Lindell M. K.** Preparedness for emergency response: guidelines for the emergency planning process // Disasters, 2003, 27 (4), 336 – 350 p. http://www2.comm.niu.edu/faculty/rholt/eocg/LLRreadUnit3APerryLindell.pdf [žiūrėta 2013 01 22]
43. **Peterson D. M., Perry R. W.** The impacts of disaster exercises on participants // Disaster Prevention and Management, 1999, vol. 8, no. 4, p. 241 – 254.
44. **Powell C.** The perception of risk and risk taking behavior: implications for incident prevention strategies // Wilderness and Environmental Medicine, 2007, no. 18, 10 – 15 p.
45. **Priest S. H.** Doing media research: an introduction / 2nd ed. – Thousand Oaks (Calif.): SAGE Publications, 2010. – 248 p.
46. **Pruskus V.** Sociologija: teorija ir praktika: mokomasis leidinys. – Vilnius: Vilniaus teisės ir verslo kolegija, 2003. – 247 p.
47. **Quarantelli E. L.** Converting disaster scholarship into effective disaster planning and managing: possibilities and limitations // International Journal of Mass Emergencies and

Disasters, 1993, vol. 11, no. 1, p. 15 – 39. http://training.fema.gov/EMIWeb/downloads/IJEMS/ARTICLES/CONVERTING%20DISASTER%20SCHOLARSHIP%20INTO%20EFFECTIVE%20DISASTER%20PLA.pdf [žiūrėta 2013 04 12]

48. **Radvanovsky R.** Critical infrastructure: homeland security and emergency preparedness. - Boca Raton (Fla.); London ; New York (N.Y.): CRC Press: Taylor and Francis Group, 2006. – 303 p.
49. **Reason J.** Achieving a safe culture: theory and practice // Work and stress, 1998, vol. 12, no. 3, p. 293 – 306. http://www.raes-hfg.com/reports/21may09-Potential/21may09-JReason.pdf [žiūrėta 2013 02 21]
50. **Rejda D.** Principles of risk management and insurance / 10th ed. – Boston (Mass): Pearson: Addison Wesley, 2008. – 748 p.
51. **Renn O.** Perception of risks // Toxicology Letters, 2004, Nr. 149, p. 405 – 413. http://ac.els-cdn.com.skaitykla.mruni.eu/S0378427403005216/1-s2.0-S0378427403005216-main.pdf?_tid=f382598c-43f3-11e3-ab7d-00000aab0f01&acdnat=1383420259_08ffe91ba298e4c7458111df841857ee [žiūrėta 2012 12 25]
52. **Renn O.** The risk handling chain // The tolerability of risk: a new framework for risk management / Frederic Bouder, David Slavin, Ragnar E. Lofstedt, editors. – London: Earthscan, 2008. – 146 p.
53. **Renn O.** Three decades of risk research: accomplishments and new chalenges // Journal of risk research, 1998, no. 1 (1), 49 – 71 p. http://paul-hadrien.info/backup/LSE/IS%20490/utile/Renn%203%20decades%20of%20risk%20research.pdf [žiūrėta 2013 05 24]
54. **Rimaitė A., Rinkevičius L.** Sociokultūrinis rizikos suvokimo konstravimas: teoriniai požiūriai ir jų taikymas tiriant viešąjį diskursą dėl genetiškai modifikuotų organizmų // Filosofija. Sociologija. – Kaunas: Lietuvos mokslų akademija Lietuvos mokslų akademijos leidykla, 2008, T. 19, Nr. 2, p. 86-96. http://www.lmaleidykla.lt/publ/0235-7186/2008/2/86-96.pdf [žiūrėta 2012 10 24]
55. **Risk and sociocultural theory: new directions and perspectives** / Edited by Deborah Lupton. – Cambridge: University Press, 1999b. – 204 p.
56. **Rohrmann B.** Risk perception, risk attitude, risk communication, risk management: a conceptual appraisal / The International Emergency Management Society, Global co-operation in emergency and disaster management – 15th TIEMS Conference booklet, 2008

http://tiems.info/dmdocuments/events/TIEMS_2008_Bernd_Rohrmann_Keynote.pdf [žiūrėta 2013 01 13]

57. **Rupšienė L.** Kokybinio tyrimo duomenų rinkimo metodologija. – Klaipėda: Klaipėdos universiteto leidykla, 2007. – 147 p.
58. **Rutherford J.** Risk management for meetings and events. – Amsterdam: Elsevier: Butterworth – Heinemann, 2008. – 354 p.
59. **Safety culture report** // A report by the international nuclear safety advisory group, 1991 http://www-pub.iaea.org/MTCD/publications/PDF/Pub882_web.pdf [žiūrėta 2013 03 16]
60. **Satyajit D.** Risk management / 3rd ed. – Singapore; Hoboken (N.J.): John Wiley, 2006. – 1327 p.
61. **Savadori L. ir kt.** Expert and public perception of risk from Biotechnology // Risk analysis, 2004, vol. 24, no. 5, p. 1289 – 1299. http://www.glerl.noaa.gov/seagrant/ClimateChangeWhiteboard/Resources/Uncertainty/Mac1/savadori04PR.pdf [žiūrėta 2013 01 04]
62. **Savage M.** Business continuity planning // Work Study, 2002, vol. 51, no. 5, p. 254 – 261.
63. **Selim G., McNamee D.** The risk management and internal auditing relationship: developing and validating a model // International Journal of Auditing, 1999, no. 3, 159 – 174 p.
64. **Sjoberg L.** Factors in risk perception // Risk Analysis, 2000, vol. 20, no. 1, p. 1 – 11. http://paul-hadrien.info/backup/LSE/IS%20490/utile/factors%20in%20risk%20perception.pdf [žiūrėta 2012-10-22]
65. **Sjoberg L.** Risk perception by the public and by experts: a dilemma in risk management // Human Ecology Review, 1999, vol. 6, no. 2, p. 1 – 9. http://www.humanecologyreview.org/pastissues/her62/62sjoberg.pdf [žiūrėta 2012 10 22]
66. **Slovic P. ir kt.** Why study risk perception? // Risk Analysis, 1982, vol. 2, no. 2, 83 – 93 p. http://sds.hss.cmu.edu/risk/articles/WhyStudyRiskPercep.pdf [žiūrėta 2012 10 22]
67. **Slovic P.** Perception of risk // Science, 1987, vol. 236, p. 280 – 285. http://www.uns.ethz.ch/edu/teach/0.pdf [žiūrėta 2012 10 22]
68. **Snedaker S.** Business Continuity and Disaster Recovery for IT Professionals. – Burlington: Elsevier, 2007. – 456 p.
69. **Steinberg R.** Governance, risk management, and compliance: it can‘t happen to us – avoiding corporate disaster while driving success. – Hoboken (N.J.): John Wiley, 2011. – 312 p.
70. **Sweeting P.** Financial enterprise risk management. – Cambridge: Cambridge University Press, 2011. – 551 p. – ISBN

71. **Taylor – Gooby P., Zinn J. O.** The current Significance of Risk // Risk in social science / Peter Taylor – Gooby, Jens O. Zinn, editors. – Oxford; New York (N. Y.): Oxford University Press, 2006. – 292 p.
72. **Tamošiūnienė R., Savčuk. O.** Risk management in Lithuanian organizations – relation with internal audit and financial statements quality // Verslas: teorija ir praktika = Business theory and practice: mokslo darbų žurnalas. – Vilnius: Vilniaus Gedimino technikos universitetas, 2007, vol. 8, no. 4, p. 204 – 213.
73. **Tidikis R.** Socialinių mokslų tyrimų metodologija. – Vilnius: Lietuvos teisės universitetas, 2003. – 626 p.
74. **Tierney K. J. ir kt**. Facing the unexpected: disaster preparedness and response in the United States. – Washington D.C.: Joseph Henry Press, 2001. – 306 p.
75. **Tolley's handbook of disaster and emergency management** / Tony Moore, Raj Lakha editors. – Amsterdam: Elsevier, 2006. – 683 p.
76. **Urniežius R.** Rizika. – Vilnius: Mintis, 2001. – 183 p.
77. **Valackienė A.** Sociologinis tyrimas: vadovėlis. – Kaunas: Technologija, 2004. – 147 p.
78. **Vancoppenolle G.** The definitive handbook of business continuity management / edited by Andrew Hiles. – Chichester: John Wiley, 2007. http://web.ebscohost.com.skaitykla.mruni.eu/ehost/ebookviewer/ebook/e000xww_246508_AN?sid=17086215-c558-405c-b2a5-7d2633072bd6@sessionmgr14&vid=3&format=EB&rid=4 [žiūrėta 2013 10 20]
79. **Weinsten N. D.** Optimistic Biases about Personal Risks // Science, 1989, vol. 246, no. 4935, 1232 – 1233 p. http://www.uic.edu/classes/psych/Health/Readings/Weinstein,%20Optimisitc%20Biases,%20Science,%201989.pdf [žiūrėta 2013-05-27]
80. **Wildavsky A., Dake K.** Theories of risk perception: who fears what and why? // Daedalus, 1990, vol. 119, no. 4, p. 41 – 60

Šablinska J. Rizikos suvokimo įtaka pasirengimo veikti ekstremaliosiose situacijose procesui: informacinių technologijų organizacijos tyrimas / Nepaprastųjų situacijų valdymo magistro baigiamasis darbas. Vadovas prof. dr. B. Pitrėnaitė – Žilėnienė. – Vilnius: Mykolo Romerio universitetas, Politikos ir vadybos fakultetas, 2013. – 95 p.

ANOTACIJA

Magistro baigiamajame darbe yra nagrinėjamas organizacijos pasiruošimas ekstremaliosioms situacijoms atsižvelgiant į vyraujantį rizikos suvokimą. Pirmoje darbo dalyje yra apžvelgiama rizikos samprata ir rizikos suvokimą aiškinantys požiūriai. Antroje dalyje yra nagrinėjamas ryšys tarp rizikos suvokimo ir jos įtakos bei svarbos pasiruošimui ekstremaliosioms situacijoms. Taip pat aptariama tęstinės veiklos plano svarba kaip pasiruošimo ekstremaliosioms situacijoms dalis. Trečioje dalyje atliekamas tyrimas, kuris atskleidžia organizacijos požiūrį į jos veiklai poveikio turinčias ekstremaliąsias situacijas ir priemones, kuriomis bandoma apsaugoti savo pažeidžiamas sritis.

Reikšminiai žodžiai: rizikos suvokimas, ekstremalioji situacija, pasiruošimas, tęstinės veiklos planas

Šablinska J. The impact of risk perception on the process of disaster preparation: the research on the organization of information technologies / Master‘s Work in Crisis management. Supervisor prof. dr. B. Pitrėnaitė – Žilėnienė. – Vilnius: Faculty of Politics and Management, Mykolas Romeris University, 2013. – 95 p.

ANOTATION

Master’s thesis analysis the organization’s preparation for emergencies according to prevailing risk perception. The first part is an overview of the risk conception and different attitudes explaining risk perception. In the second part of the work is analyzed link between risk perception and its impact on organization’s preparation for emergencies as well as the importance of risk perception. The third part is a research, which reveals organization’s approach to emergency impacts on its activities and measures that are taken to protect vulnerable areas.

Key words: risk perception, emergency management, preparedness, business continuity planning

Šablinska J. Rizikos suvokimo įtaka pasirengimo veikti ekstremaliosiose situacijose procesui: informacinių technologijų organizacijos tyrimas / Nepaprastųjų situacijų valdymo magistro baigiamasis darbas. Vadovas prof. dr. B. Pitrėnaitė – Žilėnienė. – Vilnius: Mykolo Romerio universitetas, Politikos ir vadybos fakultetas, 2013. – 95 p.

SANTRAUKA

Nagrinėjama magistro darbo tema yra aktuali, kadangi daugėjant ekstremaliosioms situacijoms didėja rizika būti paveiktiems, todėl nenutrūkstamos veiklos užtikrinimas yra reikšmingas organizacijos veiklos plėtojimui. Tačiau organizacija, nesuvokusi ir neįvertinusi jai gresiančių rizikų nesiima pasiruošiamųjų veiksmų tokių, kaip antai, tęstinės veiklos planų kūrimas. Neturint plano ir netikėtai susidūrus su ekstremaliąja situacija atsiranda nežinomybė, kuri sukuria tikimybę neatkurti savo veiklos. Būtent todėl darbe yra svarstoma **problema**, kaip organizacijos darbuotojų suvokiama rizika gali daryti įtaką jos pasiruošimą ekstremaliosioms situacijoms.

Magistro baigiamojo darbo **objektas** – rizikos suvokimas.

Tyrimo **dalykas** – rizikos suvokimo įtaka organizacijos pasiruošimui veikti ekstremaliosiose situacijose.

Darbo problema – skirtingas rizikos suvokimas lemia nevienodą požiūrį į grėsmes. Nesuvokus galimos rizikos, tikėtina, kad nebus imtasi apsisaugojimo veiksmų padėsiančių pasiruošti ekstremaliosioms situacijoms ir palengvinančių organizacijos plėtrą. Būtent todėl reikia spręsti klausimą, kokį poveikį rizikos suvokimas daro organizacijos pasiruošimo veikti ekstremaliųjų situacijų metu procesui?

Darbe buvo iškeltos trys **hipotezės**:

H_1: IT organizacijos darbuotojai kaip didžiausią poveikį turinčias organizacijos veiklai išskiria technologines grėsmes.

H_2: tiriama organizacija neturi plano aprašančio pasiruošimo veiksmus ekstremaliosioms situacijoms.

H_3: respondentai neįžvelgia tęstinės veiklos plano poreikio savo organizacijai.

Darbe buvo užsibrėžtas **tikslas** išanalizuoti ir įvertinti ar bei kokią įtaką daro rizikos suvokimas pasiruošimui ekstremaliosioms situacijoms. Šiam tikslui pasiekti buvo išskirti tokie **uždaviniai**:

1. Išanalizuoti rizikos suvokimo teorines įžvalgas ir jo svarbą ekstremaliųjų situacijų metu.
2. Nustatyti ir analizuoti priemones, kurios padėtų didinti suvokimą ir tobulinti pasiruošimą ekstremaliosioms situacijoms.

3. Tyrimu nustatyti ir įvertinti rizikos suvokimo lygį ir pasirengimo veikti ekstremaliosioms situacijoms priemones organizacijoje.
4. Pateikti tyrimo išvadas ir rekomendacijas, padėsiančias gerinti rizikos suvokimą organizacijoje.

Siekiant pasiekti iškeltą tikslą ir patvirtinti arba paneigti iškeltas hipotezes, buvo atlikta mokslinės literatūros analizė, kiekybinis ir kokybinis tyrimas. Tyrimo metu buvo orientuojamasi į organizacijos pasiruošimą, kuris apėmė tris darbe nagrinėjamas sritis, t.y. plano sukūrimą ir praktinį jo įgyvendinimą, vykdant mokymus bei plano patikrinimą vykdant pratybas.

Apklausus organizacijos darbuotojus buvo gauta informacija, atskleidžianti organizacijos suvokimą galimų rizikų atžvilgiu. Tyrimu buvo patvirtintos dvi hipotezės, kad technologinės grėsmės yra įžvelgiamos kaip didžiausią poveikį IT organizacijos veiklai turinčios ir, kad organizacija neturi plano skirto pasiruošti ekstremaliosioms situacijoms. Viena iškelta hipotezė, kad darbuotojai neįžvelgia tęstinės veiklos plano reikalingumo, buvo paneigta. Atlikto tyrimo analizė parodė, kad organizacija neskirianti dėmesio pasiruošimui, gali susidurti su sunkumais bandant atsigauti po ekstremaliosios situacijos. Organizacijoms, kurioms yra svarbu toliau vykdyti savo veiklą po ekstremaliosios situacijos siūlytina susikurti tęstinės veiklos planus, padėsiančius nusistatyti organizacijai gresiančias rizikas.

Darbo struktūra. Darbas susideda iš trijų dalių. Pirmoje darbo dalyje yra nagrinėjami įvairūs požiūriai aiškinantys rizikos suvokimą. Antroje dalyje yra nagrinėjama, kokią įtaką rizikos suvokimas turi organizacijos pasiruošimui ekstremaliosioms situacijoms. Plačiau yra apžvelgiami pasiruošimo komponentai, tokie kaip plano, padėsiančio atsigauti po ekstremaliosios situacijos sukūrimas, mokymų ir pratybų įgyvendinimas. Trečioje dalyje yra pateiktas tyrimas, kuris atskleidžia kokią svarbą organizacija suteikia pasiruošimui galimoms ekstremaliosioms situacijoms.

SUMMARY

Šablinska J. The impact of risk perception on the process of disaster preparation: the research on the organization of information technologies / Master‘s Work in Crisis management. Supervisor prof. dr. B. Pitrėnaitė – Žilėnienė. – Vilnius: Faculty of Politics and Management, Mykolas Romeris University, 2013. – 95 p.

The topic of this Master’s thesis is a relevant since the increasing number of emergencies increase the risk of being affected and assurance of continuous performance is significant to organization development. However, the organization which do not perceive and fail to assess imminence, do not take any preparation actions, such as business continuity plan. Without a plan a sudden face of emergency causes uncertainty which creates the likelihood of not recovery. Because of this **the issue** of the thesis is how risk perception may influence emergency preparation.

Three **hypothesis** were raised:

H_1: IT organization employees distinguish technological threats as having the greatest impact on organizational performance.

H_2: analyzed organization does not have a plan that describes its actions in preparation for disasters.

H_3: respondents do not envisage the need of organization business continuity plan.

The object of Master’s work – the risk perception.

The subject – the risk perception impact on organization’s disaster preparedness.

The aim of the work was to analyze and evaluate if and how risk perception influences organization’s disaster preparedness. To achieve this objective were identified these **tasks**:

1. To analyze theoretical insights of risk perception and its importance in disaster.
2. Identify and analyze measures that help to increase awareness and improve disaster preparedness.
3. Identify and evaluate the level of risk perception in organization and measures of preparedness.
4. To draw conclusion and make recommendations that improve risk perception.

In order to meet an aim and confirm or disprove raised hypothesis literature review, quantitative and quantitative researches were made. The research was focused on organization preparation which included three issues, plan establishment and its implementation through training, and testing of the plan by doing exercises.

The survey of employees revealed organization’s perception of potential risks. The study confirmed two raised hypothesis. The first one that IT organization employees distinguish

technological threats as having the greatest impact on organizational performance. And the second one that analyzed organization does not have a plan that describes its actions in preparation for disasters. The third hypothesis, that respondents do not envisage the need of organization business continuity plan, was disproved. The research showed that organization which does not focus on preparation process may encounter with difficulties when trying to recover from disaster. It is advised for organizations that are willing to pursue their activities to create business continuity plan which defines organization's underlying risks.

The structure of thesis. The work consists of three parts. The first part examines various aspects explaining risk perception. The second part deals with the impact of risk perception on organization's preparedness to emergency. Preparation components, such as plan that helps to recover after emergency, training and exercises are discussed in a wider context. The research that is made in the third part of the work reveals organizations' approach to preparation for possible emergencies.

PRIEDAI

1 PRIEDAS

ŽVALGOMOJO TYRIMO KLAUSIMYNAS

Mykolo Romerio universiteto Politikos ir vadybos fakulteto studentė atlieka tyrimą, kuriuo bus siekiama išsiaiškinti, kokį poveikį rizikos suvokimas turi organizacijos pasiruošimui ekstremaliosioms situacijoms.

Klausimynas yra anoniminis. Gauti duomenys bus panaudoti tik magistro baigiamajame darbe.

1. Kokias įžvelgiate grėsmes Jūsų organizacijai?
   1.1. Kas sąlygoja būtent tokių grėsmių išskyrimą?
2. Ar organizacija turi planą skirtą apsisaugoti nuo grėsmių?
   2.1. Jei taip, kokį?
   2.2. Jei neturi, kokios priežastys lėmė, kad organizacija neturi tokio plano?
      2.2.1. Ar įžvelgiate tokio plano poreikį? Kodėl?
3. Jei įvyktų ekstremalioji situacija, ar žinotumėte už ką esate atsakingas, ką privalote daryti?
   3.1. Iš kur Jums tai yra žinoma?
4. Ar imatės pats (pati) savarankiškai imatės kokių nors priemonių apsisaugoti nuo galimų grėsmių?
   4.1. Kas Jūs skatina taip elgtis?
5. Ar manote, organizacija yra pakankamai pasiruošusi įveikti bet kokias grėsmės?
   5.1. Kodėl taip manote ?
6. Kaip manote, ar organizacija yra pažeidžiama ir jautri įvairioms grėsmėms? Kodėl taip manote?

2 PRIEDAS

KLAUSIMYNAS
APIE RIZIKOS SUVOKIMĄ ORGANIZACIJOJE

Mykolo Romerio universiteto Politikos ir vadybos studentė atlieka tyrimą, kuriuo bus siekiama išsiaiškinti, kokį poveikį rizikos suvokimas turi organizacijos pasiruošimui ekstremaliosioms situacijoms. Prašau skirti kelias minutes anketos užpildymui.

Anketa yra anoniminė. Gauti duomenys bus panaudoti tik magistro baigiamajame darbe.

Klausimyne vartojamos sąvokos

Ekstremalioji situacija *– tai padėtis, kuri susidarė dėl ekstremaliojo įvykio ir gali sukelti didelį pavojų gyventojų gyvybei ar sveikatai, aplinkai, turtui, gali sukelti žmonių žūtį ar sužalojimus, ar gali būti padaryta kita žala.*

Ekstremalusis įvykis *- gamtinis, techninis, ekologinis ar socialinis įvykis, kuris kelia pavojų gyventojų gyvybei ar sveikatai, jų socialinėms sąlygoms, turtui ir (ar) aplinkai.*

I. Pavojų organizacijos veiklai vertinimas

1. Įvertinkite šių grėsmių galimą poveikį Jūsų organizacijos veiklai? (kur 1- jokios tikimybės iki 5 labai didelė tikimybė)

	Grėsmės	1	2	3	4	5
Gamtinės:	Potvynis					
	Gaisras					
	Sausra					
	Žemės drebėjimas					
	Audra					
	Žaibas					
	Didelis šaltis					
	Didelis karštis					
	Nuošliaužos					
	Smarkūs vėjai					
	Tornadas					
	Uraganas					
	Epidemijos, ligos					
	Gamtos užteršimas					
Technologinės:	Kompiuterio tinklų sutrikimai					
	Kompiuterio virusai					
	Įrangos gedimai					
	Telekomunikacijų sistemų sutrikimai					
	Transporto nelaimės					
	Pastato griūtis					
	Radiacinė avarija					

	Cheminio ginklo panaudojimas					
	Biologinio ginklo panaudojimas					
Žmogaus sukurtos:	Teroro aktas (pvz. kiberterorizmas)					
	Pilietiniai neramumai (streikai, protestai, riaušės)					
	Darbuotojų apgavystės					
	Turto vagystės					
	Duomenų vagystės					

2. Ar sutinkate su šiuo teiginiu: ***esu įsitikinęs (-usi), kad mano organizacija yra tinkamai pasiruošusi bet kokioms grėsmėms, todėl jos neturėtų stipriai paveikti mūsų veiklos.***

- Visiškai sutinku
- Sutinku
- Nei sutinku, nei nesutinku
- Nesutinku
- Visiškai nesutinku

3. Ar Jūs žinote, kaip elgtis, jei įvyktų ekstremalioji situacija Jums esant darbo vietoje? (Galite pasirinkti kelis atsakymo variantus)

- Taip, žinau kaip elgtis bet kokioje ekstremaliojoje situacijoje
- Ne, nežinau
- Žinau kaip elgtis tik gaisro atveju
- Žinau kaip elgtis sutrikus elektros tinklams
- Žinau kaip elgtis įvykus potvyniui
- Man to nereikia žinoti, nes už tai yra atsakingi kiti darbuotojai

II. Saugumo užtikrinimo apmokymai, aprūpinimas įranga

4. Ar sutinkate su šiuo teiginiu: ***organizacija reguliariai atnaujina įrangą, priemones skirtas apsisaugoti nuo grėsmių (pvz. nuperka naujus gesintuvus)?***

- Visiškai sutinku
- Sutinku
- Nei sutinku, nei nesutinku
- Nesutinku
- Visiškai nesutinku

5. Ar sutinkate su šiuo teiginiu: ***organizacija reguliariai vykdo apmokymus, kokių veiksmų reikėtų imtis, kad po ekstremaliojo įvykio toliau galėtumėte plėtoti savo veiklą?***

- Taip, vykdo
- Ne, nevykdo
- Nežinau

6. Jei buvo rengiami apmokymai, ar juose dalyvavote?

- Taip, dalyvavau
- Ne, nedalyvavau
- Neprisimenu

III. Tęstinės veiklos planavimas

7. Ar yra vykdoma organizacijos galimų rizikų analizė?

- Taip
- Ne
- Nežinau

8. Ar organizacija turi tęstinės veiklos planą ir/ar parengties ekstremaliosioms situacijoms planą?

- Taip, turi tęstinės veiklos planą
- Taip, turi parengties ekstremaliosioms situacijoms planą
- Taip turi abu
- Ne, neturi nei vieno
- Nežinau

9. Jei organizacija neturi tęstinės veiklos plano ir/ar parengties ekstremaliosioms situacijoms plano, Jūsų nuomone, kodėl? (Galite pasirinkti kelis atsakymo variantus)

- Per brangu, nes jo parengimas reikalauja daug finansinių išteklių
- Reikalauja specifinių žinių
- Nes toks planas nėra reikalingas, kadangi yra mažai tikėtina, kad šios rizikos paveiks organizacijos veiklą
- Per sudėtingas įgyvendinimas
- Neįeina į organizacijos tikslus

- Jis išryškina organizacijos trūkumus
- Nežinau kas tai per planas
- Kitas atsakymas (įrašykite)_____

10. Ar Jūsų organizacija turi kitą planą, kurio dėka lengvai grįžtų prie įprastinės veiklos, jei įvyktų nelaimė (gaisras, potvynis, žaibas)?

- Taip
- Ne
- Nežinau

11. Ar organizacija yra apsidraudusi nuo įvairių ekstremaliųjų įvykių?

- Taip
- Ne
- Nežinau, neturiu tokios informacijos

12. Ar Jūsų organizacija turi paskirtą žmogų/departamentą/skyrių, kuris yra atsakingas už civilinę saugą?

- Taip
- Ne
- Nežinau

13. Kokią pažeidžiamiausią organizacijos sritį galėtumėte įvardinti? (Galite pasirinkti kelis atsakymo variantus)

- Elektros tiekimo nutrūkimas
- Kompiuterių gedimai
- Silpna kompiuterinės įrangos apsauga
- Nepatikima pastato konstrukcija
- Prasta priešgaisrinė įranga
- Vykdoma veikla
- Nėra pažeidžiamų sričių
- Kitas atsakymas (įrašykite) _____

14. Ar, Jūsų nuomone, organizacijai reikalingas dokumentas (planas, taisyklės, procedūros), kuriame būtų reglamentuoti veiksmai per ir po ekstremaliojo įvykio?

- Taip
- Ne
- Neturiu nuomonės

15. Jei toks dokumentas reikalingas, kas turėtų būti jame numatyta? (Galite pasirinkti kelis atsakymo variantus)

- Veiksmai, ką reikėtų daryti ekstremaliosios situacijos metu
- Organizacijai aktualios grėsmės ir jų tikimybės
- Veiksmai, kurių reikėtų imtis grėsmių poveikiui sumažinti
- Asmenys, atsakingi už tam tikrą saugumo sritį
- Reguliarūs apmokymai, padėsiantys nepasimesti tokioje situacijoje
- Tarpusavio komunikacijos schemos
- Kitas atsakymas (įrašykite)_____

16. Jūsų amžius:

- Iki 25 metų
- 26 – 35 metai
- 36 – 45 metai
- 46 ar daugiau metų

17. Jūsų išsilavinimas:

- Pagrindinis
- Vidurinis
- Specialusis vidurinis
- Aukštesnysis
- Nebaigtas aukštasis
- Aukštasis

18. Kokia Jūsų darbo patirtis šioje organizacijoje?

- Iki 1 metų
- 1 – 5 metai
- 6 - 10
- 11 ar daugiau metų

3 PRIEDAS

ANALITINIŲ TURINIO VIENETŲ IŠSKYRIMAS

Respondentų pasisakymai	Tema / apibendrinimas
A ANKETA	
A1.1.-1 Mūsų pačių patirtis	Grėsmių išskyrimą skatinantis veiksnys
A3-2 Nežinau	Informacijos dėl plano stoka
A4-3 Ne	Žinios kaip elgtis
A5-4 Lojalumas A5-5 Atsakomybė įmonei, kurioje dirbu	Veiksniai skatinantys savarankiškai saugotis
A6-6 Žinau, nes jau vieną tokią grėsmę įveikėme	Organizacijos pasiruošimas įveikti grėsmes
A7-7 Taip, kiekviena organizacija yra pažeidžiama ir jautri grėsmėms, mūsų įmonė – ne išimtis.	Organizacijos pažeidžiamumas
B ANKETA	
B1.1.-1 Tokių atvejų kol kas nepasitaikė, bet mano nuomone, minėtos grėsmės yra tikrai didelės.	Grėsmių išskyrimą skatinantis veiksnys
B3-2 Taip. Apsaugotas vidinis tinklas, ugniasienė, patalpų apsauga, ribojamas patekimas į patalpas.	Organizacijos turimas planas
B3.2.1.-3 Žinoma. Jeigu tokio nebūtų – padidėtų grėsmių tikėtinumas.	Plano poreikis
B4-4 Natūraliai	Žinios kaip elgtis
B5-5 Duomenų svarbumas	Veiksniai skatinantys savarankiškai saugotis
B6-6 Taip. Nes tam yra skirti specialistai, kurie už tai atsakingi.	Organizacijos pasiruošimas įveikti grėsmes
B7-7 Pažeidžiama. Pažeidžiami netgi bankai turintys prevencijos skyrius su keletu ar keliolika darbuotojų	Organizacijos pažeidžiamumas
C ANKETA	
C1.1.-1 Žiniasklaida, C1.1-2 Panašių organizacijų patirtis.	Grėsmių išskyrimą skatinantis veiksnys
C3-3 Nežinau	Informacijos dėl plano stoka
C3.2.1.-4 Toks planas yra gerai, kad apsisaugoti nuo grėsmių	Plano poreikis

Lentelės tęsinys kitame puslapyje

Lentelės tęsinys

Respondentų pasisakymai	Tema / apibendrinimas
C4-5 Taip. Iš saugumo technikos taisyklių	Žinios kaip elgtis
C5-6 Žmogiškasis faktorius	Veiksniai skatinantys savarankiškai saugotis
C6-7 Organizacija ilgai gyvuoja, todėl turi didelę patirtį.	Organizacijos pasiruošimas įveikti grėsmes
C7-8 Visos organizacijos yra pažeidžiamos ir jautrios. Vienos mažiau, kitos daugiau.	Organizacijos pažeidžiamumas
D ANKETA	
D1.1.-1 Patirtis, D1.1.-2 Žiniasklaida, D1.1.-3 Konkurencija rinkoje	Grėsmių išskyrimą skatinantis veiksnys
D3- 4 Nežinau	Informacijos dėl plano stoka
D3.2.1.-5 Taip, protinga yra saugoti ir rūpintis savo resursais	Plano poreikis
D4- 6 Taip, iš darbuotojo nuostatos	Žinios kaip elgtis
D5-7 Geras būdas D5-8 Suinteresuotumas nekenkti organizacijai, kurioje dirbu.	Veiksniai skatinantys savarankiškai saugotis
D6-9 Nežinau. Apie tokius dalykus informacija nėra skleidžiama organizacijos viduje tarp darbuotojų	Organizacijos pasiruošimas įveikti grėsmes
D7-10 Organizacija yra rinkos dalis, todėl pokyčiai rinkoje įtakoja organizaciją. D7-11 Organizacija turi santykinę apsaugą nuo kai kurių grėsmių, bet ne nuo visų įmanomų tam, kad išlaikytų status quo.	Organizacijos pažeidžiamumas
E ANKETA	
E1.1.-1 Asmeninė nuomonė	Grėsmių išskyrimą skatinantis veiksnys
E3-2 Nežinau	Informacijos dėl plano stoka
E3.2.1.-3 Galbūt būtų neblogai, tačiau jis, mano nuomone, nėra būtinas.	Plano poreikis

Lentelės tęsinys kitame puslapyje

Lentelės tęsinys

Respondentų pasisakymai	Tema / apibendrinimas
E4-4 Taip, iš bendro išprusimo	Žinojimas kaip elgtis
E5-5 Noras apsisaugoti nuo galimos žalos	Veiksniai skatinantys savarankiškai saugotis
E6-6 (...), nes dirba daug specialistų	Organizacijos pasiruošimas įveikti grėsmes
E7-7 Kai kurioms grėsmėms jautri	Organizacijos pažeidžiamumas
F ANKETA	
F1.1-1 Patirtis	Grėsmių išskyrimą skatinantis veiksnys
F3- 2 Nežinau	Informacijos dėl plano stoka
F3.2.1-3 Taip, nes užtikrina veiklos tęstinumą	Plano poreikis
F4-4 Ne	Žinojimas kaip elgtis
F5-5 Noras apsaugoti save ir kolegas nuo nelaimės F5-6 Noras apsaugoti įmonę nuo potencialių nuostolių.	Veiksniai skatinantys savarankiškai saugotis
F6-7 Taip, nes kiekviena solidi įmonė rūpinasi savo reputacija F6-8 Veiklos tęstinumo užtikrinimas net ekstremaliomis aplinkybėmis	Organizacijos pasiruošimas įveikti grėsmes
F7-9 Manau, kad bendrovė yra pažeidžiama atsižvelgiant į teikiamų paslaugų pobūdį.	Organizacijos pažeidžiamumas
G ANKETA	
G1.1.-1 Asmeninė nuomonė	Grėsmių išskyrimą skatinantis veiksnys
G3-2 Nežinau	Informacijos dėl plano stoka
G4-3 Ne	Žinojimas kaip elgtis
G5-4 Patirtis	Veiksniai skatinantys savarankiškai saugotis

Lentelės tęsinys kitame puslapyje

Lentelės tęsinys

Respondentų pasisakymai	Tema / apibendrinimas
G6- 5 Nežinau	Organizacijos pasiruošimas įveikti grėsmes
G7-6 Pažeidžiama. Pažeidžiami netgi bankai turintys prevencijos skyrius su keletu ar keliolika darbuotojų	Organizacijos pažeidžiamumas
H ANKETA	
H1.1.-1 patirtis	Grėsmių išskyrimą skatinantis veiksnys
H3-2 ne, nes nebuvo precedento	Informacijos dėl plano stoka
H3.2.1.-3 Taip. Įvykus minėtoms grėsmėms turi būti atsakingas asmuo, kuris žinotų kaip elgtis tokioje situacijoje.	Plano poreikis
H4-4 Ne	Žinojimas kaip elgtis
H5-5 Sveikas protas	Veiksniai skatinantys savarankiškai saugotis
H6-6 Neturiu informacijos apie panašaus plano buvimą	Organizacijos pasiruošimas įveikti grėsmes
H7-7 Taip. Didžioji dalis darbų vykdoma virtualioje erdvėje, todėl bet koks sutrikimas stabdo darbą, prarandama informacija ar net ta, tikro laikotarpio darbo rezultatai.	Organizacijos pažeidžiamumas
I INTERVIU	
I3-1 Taip. Tinklo apsaugos sistemos, ribojamas patekimas į patalpas.	Informacijos dėl plano stoka
I3.2.1.-2 Taip, kadangi organizacija įdėjus daug pastangų, jog šios grėsmės neįvyktų.	Plano poreikis
I4-3 Taip, iš darbo saugos dokumento	Žinojimas kaip elgtis
I5-4 Organizacijos duomenų svarba	Veiksniai skatinantys savarankiškai saugotis

Lentelės tęsinys kitame puslapyje

Lentelės tęsinys

Respondentų pasisakymai	Tema / apibendrinimas
I6-5 Taip, kadangi organizacija įdėjus daug pastangų, jog šios grėsmės neįvyktų.	Organizacijos pasiruošimas įveikti grėsmes
I7-6 Jautri, tačiau nepažeidžiama, nes turim planą, kuriuo vadovaujantis grėsmių tikimybė minimali.	Organizacijos pažeidžiamumas
J ANKETA	
J1.1.-1 Technikos nusidėvėjimas	Grėsmių išskyrimą skatinantis veiksnys
J3-2 Nežinau	Informacijos dėl plano stoka
J3.2.1.-3 Ne	Plano poreikis
J5-4 Taip. Baimė prarasti, sugadinti turimą informaciją, duomenis, įmonės turtą ir t.t.	Veiksniai skatinantys savarankiškai saugotis
J6-5 Taip, dirba profesionalūs J6-6 apmokyti darbuotojai.	Organizacijos pasiruošimas įveikti grėsmes
J7-7 Nei viena organizacija nėra apsaugota nuo grėsmių, tačiau kiekviena stengiasi, kad tos grėsmės neįvyktų.	Organizacijos pažeidžiamumas
K ANKETA	
K1.1.-1 Patirtis	Grėsmių išskyrimą skatinantis veiksnys
K3.1-2 Rašytinio plano nėra, tiesiog stiprinamos grėsmingos vietos.	Organizacijos turimas planas
K3.2-3 Tikimybės ir rizikos faktorius nepakankamas. Be to, kas liečia infrastruktūros kiek žinau toks planas atsiras	Plano neturėjimo priežastys
K3.2.1.-4 Reikalingas, nes jis padės geriau valdyti kritines vietas	Plano poreikis
K5-5 Taip. Stipriname kompetencijas, K5-6 Optimizuojame procesus.	Veiksniai skatinantys savarankiškai saugotis

Lentelės tęsinys kitame puslapyje

Lentelės tęsinys

Respondentų pasisakymai	Tema / apibendrinimas
K1.1.-1 Patirtis	Grėsmių išskyrimą skatinantis veiksnys
K6-7 Vidutiniškai	Organizacijos pasiruošimas įveikti grėsmes
K7-8 Ir taip ir ne. Esant dideliam norui bet kokios organizacijos apsaugas šiais laikais galima, jeigu ne neutralizuoti, bet bent sustabdyti įmonės darbą.	Organizacijos pažeidžiamumas
L ANKETA	
L1.1.-1 Saugumo spragos L1.1.-2 Didelės tarptautinės kompanijos.	Grėsmių išskyrimą skatinantis veiksnys
L3.2-3 Neturi. Neįžvelgiamos grėsmės ir pasekmės.	Organizacijos turimas planas
L3.2.1.-4 Taip	Plano poreikis
L3.2.-5Neįžvelgiamos grėsmės ir pasekmės	Plano stokos priežastys
L5-6 Laikausi standartinių saugumo normų	Veiksniai skatinantys savarankiškai saugotis
L7-7 Galima (vadinti pažeidžiama), nes kol kas nevaldome proceso.	Organizacijos pažeidžiamumas

4 PRIEDAS

ŽVALGYBINIO TYRIMO RESPONDENTŲ ATSAKYMAI

1. Kokias įžvelgiate grėsmes Jūsų organizacijai?

Respondentas Nr. 1: protų nutekėjimas, virusai, kompiuteriniai tinklų sutrikimai, duomenų iškraipymai, duomenų praradimas, konkurentai, duomenų vagystė.

Respondentas Nr. 2: įrangos vagystė, virusai, duomenų praradimas, kompiuteriniai tinklų sutrikimai, techniniai gedimai, duomenų vagystė.

Respondentas Nr. 3: techniniai gedimai, virusai, kompiuteriniai tinklų sutrikimai.

Respondentas Nr. 4: virusai, duomenų vagystės.

Respondentas Nr. 5: kompiuteriniai tinklų sutrikimai, duomenų iškraipymai, duomenų praradimas, techniniai gedimai, duomenų vagystė.

Respondentas Nr. 6: duomenų praradimas, techniniai gedimai.

Respondentas Nr. 7: virusai, duomenų iškraipymai, duomenų praradimas, konkurentai, duomenų vagystė.

Respondentas Nr. 8: : duomenų vagystė, kompiuteriniai tinklų sutrikimai, duomenų praradimas, techniniai gedimai,.

Respondentas Nr. 9: : virusai, kompiuteriniai tinklų sutrikimai.

Respondentas Nr. 10: : kompiuteriniai tinklų sutrikimai, virusai, duomenų praradimas, techniniai gedimai.

Vadovai:

Respondentas Nr. 11: techniniai gedimai, duomenų praradimas, kompiuteriniai tinklų sutrikimai.

Respondentas Nr. 12: duomenų praradimas, konkurentai, virusai.

1.1. Kas sąlygoja tokių grėsmių išskyrimą?

Respondentas Nr. 1: mūsų pačių patirtis.

Respondentas Nr. 2: tokių atvejų kol kas nepasitaikė, bet mano nuomone, minėtos grėsmės yra tikrai didelės.

Respondentas Nr. 3: žiniasklaida, panašių organizacijų patirtis.

Respondentas Nr. 4: patirtis, žiniasklaida, konkurencija rinkoje.

Respondentas Nr. 5: asmeninė nuomonė.

Respondentas Nr. 6: patirtis.

Respondentas Nr. 7: asmeninė nuomonė.

Respondentas Nr. 8: patirtis.

Respondentas Nr. 9: -

Respondentas Nr. 10: technikos nusidėvėjimas.

Vadovai:

Respondentas Nr. 11: patirtis.

Respondentas Nr. 12: saugumo spragos ir didelės tarptautinės kompanijos.

2. Ar organizacija turi planą skirtą apsisaugoti nuo grėsmių?

2.1. Jei taip, kokį?

Respondentas Nr. 1: nežinau

Respondentas Nr. 2 : taip. Apsaugotas vidinis tinklas, ugniasienė, patalpų apsauga, ribojamas patekimas į patalpas.

Respondentas Nr. 3: nežinau

Respondentas Nr. 4: nežinau

Respondentas Nr. 5: nežinau

Respondentas Nr. 6: nežinau

Respondentas Nr. 7: nežinau

Respondentas Nr. 8: ne

Respondentas Nr. 9: taip. Tinklo apsaugos sistemos, ribojamas patekimas į patalpas.

Respondentas Nr. 10: nežinau

Vadovai:

Respondentas Nr. 11: rašytinio plano nėra, tiesiog stiprinamos grėsmingos vietos.

Respondentas Nr. 12: neturi

2.2. Jei neturi, kokios priežastys lėmė, kad organizacija neturi tokio plano?

Respondentas Nr. 1: -

Respondentas Nr. 2: -

Respondentas Nr. 3: -

Respondentas Nr. 4: -

Respondentas Nr. 5: -

Respondentas Nr. 6: -

Respondentas Nr. 7: -

Respondentas Nr. 8: nebuvo precedento

Respondentas Nr. 9: -

Respondentas Nr. 10: -

Vadovai:

Respondentas Nr. 11: tikimybės ir rizikos faktorius nepakankamas. Be to, kas liečia infrastruktūros kiek žinau toks planas atsiras.

Respondentas Nr. 12: neįžvelgiamos grėsmės ir pasekmės

2.2.1. Ar įžvelgiate tokio plano poreikį? Kodėl?

Respondentas Nr. 1: -

Respondentas Nr. 2.: žinoma. Jeigu tokio nebūtų – padidėtų grėsmių tikėtinumas.

Respondentas Nr. 3: toks planas yra gerai, kad apsisaugoti nuo grėsmių

Respondentas Nr. 4: taip, protinga yra saugoti ir rūpintis savo resursais, nes nuo jų priklauso tolimesnė organizacijos padėtis.

Respondentas Nr. 5: galbūt būtų neblogai, tačiau jis, mano nuomone, nėra būtinas.

Respondentas Nr. 6: taip, nes užtikrina veiklos tęstinumą.

Respondentas Nr. 7:-

Respondentas Nr. 8: taip. Įvykus minėtoms grėsmėms turi būti atsakingas asmuo, kuris žinotų kaip elgtis tokioje situacijoje.

Respondentas Nr. 9: taip, kadangi be jo stipriai išaugtų grėsmių įvykimo tikimybė

Respondentas Nr. 10: ne

Vadovai

Respondentas Nr.11: reikalingas, nes jis padės geriau valdyti kritines vietas

Respondentas Nr. 12: taip

3. Jei įvyktų ekstremalioji situacija, ar žinotumėte už ką esate atsakingas, ką privalote daryti? Iš kur Jums tai yra žinoma?

Respondentas Nr. 1: ne

Respondentas Nr. 2: taip. Natūraliai.

Respondentas Nr. 3: taip, iš saugumo technikos taisyklių.

Respondentas Nr. 4: taip, darbuotojo nuostatos.

Respondentas Nr. 5: taip, iš bendro išprusimo.

Respondentas Nr. 6: ne

Respondentas Nr. 7: ne

Respondentas Nr. 8: ne

Respondentas Nr. 9: taip, iš darbų saugos dokumento.

Respondentas Nr.10: taip, kiekvienas turime tam tikras pareigybes darbe

Vadovai:

Respondentas Nr.11:-

Respondentas Nr.12:-

4. Ar imatės pats (pati) savarankiškai imatės kokių nors priemonių apsisaugoti nuo galimų grėsmių?

4.1. Kas Jūs skatina taip elgtis?

Respondentas Nr. 1: taip. Lojalumas ir atsakomybė įmonei, kurioje dirbu.

Respondentas Nr. 2: taip. Duomenų svarbumas.

Respondentas Nr. 3: taip. Žmogiškasis faktorius.

Respondentas Nr. 4: taip. Geras būdas ir suinteresuotumas nekenkti organizacijai, kurioje dirbu.

Respondentas Nr. 5: taip. Noras apsisaugoti nuo galimos žalos.

Respondentas Nr. 6: taip. Noras apsaugoti save ir kolegas nuo nelaimės ir įmonę nuo potencialių nuostolių.

Respondentas Nr. 7: taip. Patirtis.

Respondentas Nr. 8: taip. Sveikas protas.

Respondentas Nr. 9: taip. Organizacijos duomenų svarba.

Respondentas Nr. 10: taip. Baimė prarasti, sugadinti turimą informaciją, duomenis, įmonės turtą ir t.t.

Vadovai

Respondentas Nr. 11: taip. Stipriname kompetencijas, optimizuojame procesus.

Respondentas Nr. 12: taip, laikausi standartinių saugumo normų.

5. Ar manote, organizacija yra pakankamai pasiruošusi įveikti bet kokias grėsmės?

5.1. Kodėl taip manote ?

Respondentas Nr. 1: taip. Žinau, nes jau ne vieną tokią grėsmę įveikėme.

Respondentas Nr. 2: taip. Nes tam yra skirti specialistai, kurie už tai atsakingi.

Respondentas Nr. 3: taip. Organizacija ilgai gyvuoja, todėl turi didelę patirtį.

Respondentas Nr. 4: nežinau. Apie tokius dalykus informacija nėra skleidžiama organizacijos viduje tarp darbuotojų.

Respondentas Nr. 5: taip, nes dirba daug specialistų.

Respondentas Nr. 6: taip, nes kiekviena solidi įmonė rūpinasi savo reputacija ir veiklos tęstinumo. užtikrinimu net ekstremaliomis aplinkybėmis

Respondentas Nr. 7: nežinau.

Respondentas Nr. 8: ne. Neturiu informacijos apie panašaus plano buvimą.

Respondentas Nr. 9: taip, kadangi organizacija įdėjus daug pastangų, jog šios grėsmės neįvyktų.

Respondentas Nr. 10: taip, dirba profesionalūs ir apmokyti darbuotojai.

Vadovai:

Kaip vertinate organizacijos pasiruošimą bet kokioms grėsmėms?

Respondentas Nr. 11: vidutiniškai

Respondentas Nr. 12: teigiamai

6. Kaip manote, ar organizacija yra pažeidžiama ir jautri įvairioms grėsmėms? Kodėl taip manote?

Respondentas Nr. 1: taip, kiekviena organizacija yra pažeidžiama ir jautri grėsmėms, mūsų įmonė – ne išimtis.

Respondentas Nr. 2: nepažeidžiama, tačiau visko gali nutikti.

Respondentas Nr. 3: visos organizacijos yra pažeidžiamos ir jautrios. Vienos mažiau, kitos daugiau.

Respondentas Nr. 4: organizacija ra rinkos dalis, todėl pokyčiai rinkoje įtakoja organizaciją. Organizacija turi santykinę apsaugą nuo kai kurių grėsmių, bet ne nuo visų įmanomų tam, kad išlaikytų status quo.

Respondentas Nr. 5: kai kurioms grėsmėms jautri.

Respondentas Nr. 6: manau, kad bendrovė yra pažeidžiama atsižvelgiant į teikiamų paslaugų pobūdį.

Respondentas Nr. 7: pažeidžiama. Pažeidžiami netgi bankai turintys prevencijos skyrius su keletu ar keliolika darbuotojų

Respondentas Nr. 8: taip. Didžioji dalis darbų vykdomas virtualioje erdvėje, todėl bet koks sutrikimas stabdo darbą, prarandama informacija ar net ta, tikro laikotarpio darbo rezultatai.

Respondentas Nr. 9: jautri, tačiau nepažeidžiama, nes turim planą, kuriuo vadovaujantis grėsmių tikimybė minimali.

Respondentas Nr. 10: nei viena organizacija nėra apsaugota nuo grėsmių, tačiau kiekviena stengiasi, kad tos grėsmės neįvyktų.

Vadovai:

Respondentas Nr. 11: ir taip ir ne. Esant dideliam norui bet kokios organizacijos apsaugas šiais laikais galima jeigu ne neutralizuoti, bet bent sustabdyti įmonės darbą.

Respondentas Nr. 12: galima (vadinti pažeidžiama), nes kol kas nevaldome proceso.

5 PRIEDAS

GRĖSMIŲ IŠSKYRIMO PRIEŽASTYS

Siekiant nustatyti, kas lemia tokių grėsmių pasirinkimą buvo įvardintos kelios priežastys (žr. 1 lent.).

1 lentelė. Grėsmių išskyrimo priežastys

Teiginys	Potemė	Tema
Mūsų pačių patirtis (A1.1.-1)	Patirtis	Veiksniai lemiantys grėsmių išskyrimą
Panašių organizacijų patirtis (C1.1-2)		
Patirtis (D1.1.-1)		
Patirtis (F1.1-1)		
Patirtis (H1.1.-1)		
Patirtis (K1.1.-1)		
Žiniasklaida (D1.1.-2)	Išoriniai veiksniai	
Žiniasklaida (C1.1.-1)		
Konkurencija rinkoje (D1.1.-3)		
Asmeninė nuomonė (G1.1.-1)	Asmeninė nuomonė	
Asmeninė nuomonė (E1.1.-1)		
Saugumo spragos (L1.1.-1)	Vidinės organizacijos priežastys	
Technikos nusidėvėjimas (J1.1.-1)		

Kiekvienas respondentas suvokia skirtingas organizacijai kylančias grėsmes. Šis suvokimas yra grindžiamas daugelio veiksnių. Siekiant geriau suprasti kas skatina šių grėsmių išskyrimą svarbu žinoti kas tam turi poveikio. Apklaustieji organizacijos darbuotojai kaip dažniausią iš priežasčių, prisidedančią prie tam tikrų grėsmių įvardijimo išskyrė patirtį. Tai buvo arba pačių respondentų patirtis nagrinėjamoje organizacijoje (A1.1.-1; D1.1.-1; F1.1.-1; H1.1.-1; K1.1.-1) arba kitų, panašia veikla užsiimančių organizacijų patirtis (C1.1.-2).

Ne ką mažiau svarbesniais galima laikyti išorinius veiksnius, turinčius įtakos vienokių arba kitokių grėsmių išskyrimui. Šiuo atveju tai yra žiniasklaidos (D1.1.-2; C1.1-1) įtaka ir konkurentų, veikiančių rinkoje, įvertinimas (D1.1-3).

Tačiau svarbu yra įvertinti ne tik išorines priežastis, bet ir vidines tokias, kurias organizacija gali bent šiek tiek paveikti pati. Viena iš tokių priežasčių respondento buvo įvardinta kaip „technikos nusidėvėjimas“ (J1.1-1). Įvykus ekstremaliajai situacijai ir turint nusidėvėjusias technologijas galima patirti nemažai nuostolių, tiek prarandant vertingą informaciją, kurią gali būti sudėtinga atkurti, tiek parardant patį turtą. Kita priežastis yra organizacijoje vyraujančios „saugumo spragos“ (L1.1-1). Nepaisant to, kad yra laikomasi saugumo priemonių, vis dėlto esantys trūkumai padidina grėsmių tikimybę.

Rezultatai rodo, kad rizikos suvokimą formuoja daug įvairių faktorių. Vienokių ar kitokių grėsmių išskyrimą formuoja respondentų suvokimas apie jų atsiradimo riziką. Išorines priežastis

valdyti yra sunkiau, tačiau žinant organizacijos viduje egzistuojančias spragas galima tobulinti esamus trūkumus ir išvengti tam tikrų grėsmių tikimybės.