VILNIAUS UNIVERSITETAS
EKONOMIKOS IR VERSLO ADMINISTRAVIMO FAKULTETAS

STRATEGINIS INFORMACINIŲ SISTEMŲ VALDYMAS

Deimantė Jotautaitė

MAGISTRO BAIGIAMASIS DARBAS

KIBERNETINĖS RIZIKOS VALDYMO ĮTAKA ĮMONIŲ VEIKLOS REZULTATAMS	IMPACT OF CYBER RISK MANAGEMENT ON COMPANIES‘ PERFORMANCE RESULTS

Darbo vadovas doc. dr. Mindaugas Krutinis

Vilnius, 2022

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

ĮVADAS

Darbo temos aktualumas. Šiuolaikiniame pasaulyje organizacijos plačiai naudoja informacinių technologijų (toliau - IT) sistemas, kad apdorotų informaciją, užtikrintų efektyvesnį sprendimų priėmimo procesą bei padėtų kurti pridėtinę vertė ir įgyvendinti kitus įmonės užsibrėžtus tikslus. Dabar IT yra neatsiejama organizacijų verslo procesų užtikrinimo priemonė. Įmonės tampa vis labiau priklausomos nuo IT, todėl kibernetinės rizikos valdymas tampa vis svarbesnis, nes atlieka ypatingą vaidmenį saugant organizacijos informacijos turtą bei pačią organizaciją ir jos klientų duomenis.

IT įmonėse daro didelę įtaką įmonės rezultatams - pirma, IT gerina prekių ir paslaugų kokybę, jų koordinavimą. Antra, įmonės pasitelkdamos verslo analitikos sistemas, IT pagalba gali priimti efektyvesnius įvairaus valdymo lygmens, net ir strateginius sprendimus, kurie turi įtakos įmonės finansiniams ir ne finansiniams rezultatams. Didėjantis IT naudojimas neabejotinai didina ir kibernetinio saugumo reikšmę organizacijose, todėl rizikos valdymo procesas pirmiausia turėtų būti laikomas ne vien technine funkcija, o esmine organizacijos valdymo funkcija.

Dėl dinamiškos verslo aplinkos ir kintančių poreikių, kuomet įmonėse vis daugiau taikomi IT sprendimai, o įmonių veikla tampa dar labiau priklausoma nuo skaitmeninės informacijos, kyla ir didesnė rizika tapti pažeidžiamiems kibernetinėje erdvėje. Nacionalinėje Lietuvos kibernetinio saugumo strategijoje įvardijama, kad kibernetinių incidentų skaičius kasmet padidėja dešimtadaliu, incidentai vis sudėtingesni ir kompleksiški bei meta iššūkį dabartiniams rizikos valdymo metodams. Tinkamai ir laiku nesuvaldytas kibernetinis incidentas gali turėti neigiamos įtakos organizacijos veiklos tęstinumui, reputacijai, finansiniams ir ne finansiniams įmonės rezultatams. Kibernetinės atakos vyksta dažniau ir tampa vis pavojingesnės. Nacionalinio kibernetinio saugumo centro teigimu, kibernetinės atakos auka gali tapti kiekviena įmonė, nepriklausomai nuo dydžio, vykdomos veiklos ar naudojamų kibernetinio saugumo priemonių modernumo. Tačiau, Lietuvos statistikos departamento skelbiami duomenys rodo, kad kuo mažesnė įmonė, tuo mažiau dėmesio ji skiria saugumo sistemoms internetinėje erdvėje diegti.

Finansų sektorius yra vienas iš labiausiai kibernetinių atakų paveiktų sektorių. Finansinių technologijų įmonės yra finansų sektoriaus variklis. Nors jų siūlomi įvairūs finansiniai sprendimai technologijų pagrindu skatina viso finansų sektoriaus vystymąsi, bet kartu atneša ir didesnį kibernetinės rizikos poveikį. Visuomenėje vis dar nėra stipraus pasitikėjimo finansinių

technologijų sektoriumi. Tai gali lemti jo bei visos finansų sistemos tolimesnę raidą, todėl kibernetinio saugumo tyrimų aktualumas vis didėja.

Šiuo darbu siekiama išsiaiškinti kibernetinės rizikos valdymo įtaką įmonių veiklos rezultatams bei įvardinti svarbiausius veiksnius, lemiančius organizacijos kibernetinio saugumo pasirengimą. Kibernetinės rizikos yra lanksčios ir nuolat kintančios, o jų valdymas yra svarbus norint išlaikyti verslo infrastuktūrą ir sėkmę tiek dabar, tiek ateityje. Taip pat svarbu paminėti, jog tema aktuali ir moksline prasme dėl nepakankamo temos ištirtumo ne tik Lietuvos, bet ir platesniu mastu, todėl šis darbas galėtų tapti indėliu į akademinį pasaulį stipresnio kibernetinio saugumo valdymo poveikio įmonių veiklos rezultatams išnagrinėjimo prasme. Šis darbas galėtų būti indėlis į geresnį pasitikėjimą Finansinių technologijų sektoriumi, nes šios įmonės yra atliekamo tyrimo vienetai.

Temos ištyrimo lygis. IT saugos rizikų valdymas ir įtaka įmonių veiklai bei verslo procesams yra daugiau išanalizuota užsienio mokslininkų, tačiau tema daugiau išnagrinėta kibernetinio saugumo, kibernetinių incidentų sąvokų ir klasifikacijos ar rizikos valdymo prasme. Bendrai kibernetinis saugumas bei jo įtaka informacinei visuomenei, kurios vystymasis pagrįstas IT revoliucija ir inovacijomis, aptariami Canongia ir Mandarino (2012) mokslinių darbų rinkinyje. Kibernetinio saugumo svarba įmonėse nagrinėjama Kaplan, Bailey, O'Halloran, Marcus ir Rezek (2015) knygoje ir James (2018) straipsniuose. IT saugos rizikų valdymas bei įtaka įmonių verslo procesams nagrinėjama Hernadez ir Schou (2014) bei Moşteanu (2020) ir Copeland (2017) tyrimuose. Kibernetino saugumo efektyvumą įmonėje sustiprinantys veiksniai įvardijami Skrypnikov, Kozlov, Denisenko, Saranov, Kuznecova ir Savchenko (2020) moksliniame straipsnyje. Temai atskleisti naudingi Lietuvos autorių moksliniai šaltiniai: Grincevičiaus (2019) aptartas kibernetinio valdymo saugumo gerinimas, Kuklytės ir Ūso (2017) aprašytos kibernetinių incidentų formos, IT saugos rizikos identifikavimo ir vertinimo tema aptarta Jevsejev (2020) bei Janieliūnienės ir Davidavičienės (2013) straipsniuose.

Nors kibernetinė rizika ir kibernetinis saugumas tampa vis aktualesnė tema užsienio moksliniuose tyrimuose, Lietuvos mokslinėje literatūroje kibernetinis saugumas daugiau ištirtas tik valstybės mastu. Kibernetinės rizikos valdymo įtaką įmonių veiklos rezultatams nėra plačiai išnagrinėta tema Lietuvos mokslinėje literatūroje, todėl tai leidžia užtikrinti šio darbo aktualumą ir naujumą akademiniu lygmeniu.

Problema. Kokią įtaką kibernetinės rizikos valdymas turi įmonių veiklos rezultatams?

Tyrimo objektas. Kibernetinis saugumas, kibernetinio saugumo veiksniai.

Darbo tikslas. Įvertinti kibernetinės rizikos valdymo įtaką įmonių veiklos rezultatams.

Uždaviniai:

1. Atlikus mokslinių šaltinių analizę aprašyti pagrindinius teorinius aspektus susijusius kibernetine rizika - pateikti kibernetinės rizikos ir kibernetinio saugumo sampratą bei komponentus, įvardinti kibernetinių incidentų tipus.
2. Mokslinės literatūros analizės pagrindu apžvelgti kibernetinio saugumo veiksnius, kibernetinės rizikos valdymo svarbą įmonės rezultatams ir išsiaiškinti labiausiai kibernetinės rizikos veikiamus sektorius.
3. Remiantis moksliniais straipsniais ir teorinėmis įžvalgomis suformuoti tyrimo metodologiją ir jos pagrindu atlikti tyrimą.
4. Išanalizavus atlikto tyrimo rezultatus pateikti rekomendacijas kaip sustiprinti kibernetinės rizikos valdymo veiksnius, kurie prisidėtų prie įmonių saugumo ir veiklos rezultatų gerinimo.

Darbo metodai. Analizuojant teorinius ir metodologinius temos aspektus naudojama mokslinės literatūros ir tyrimų analizė, grafinė duomenų bei palyginamoji analizė. Taip pat naudojami duomenų grupavimo, lyginimo, informacijos sisteminimo bei aprašomasis metodai.

Darbo tyrimui naudojamas kiekybinis tyrimo metodas – apklausa, suformuota remiantis atliktų mokslinių tyrimų pagrindu, kuri padėtų išsiaiškinti kokie veiksniai prisideda prie įmonių kibernetinio saugumo pasirengimo bei jo poveikio įmonių veiklos rezultatams.

Tyrimo rezultatų analizei naudojama statistinė analizė - aprašomoji statistika, hipotezių tikrinimo ir ryšių tarp kintamųjų metodai - koreliacinė ir regresinė analizė.

Darbo struktūra.

Magistro darbą sudaro 87 puslapiai (su priedais), 97 literatūros šaltiniai.

Pirmajame darbo skyriuje pateikiami pagrindiniai kibernetinės rizikos teoriniai aspektai - įvardijama kibernetinės rizikos sąvoka, pateikiama kibernetinių incidentų klasifikacija, paaiškinama kibernetinio saugumo sąvoka ir pagrindiniai komponentai. Taip pat pateikiami organizacijos kibernetinio saugumo pasirengimą skatinantys veiksniai. Pristatoma kibernetinės rizikos valdymo svarba įmonės veiklos rezultatams bei aprašomi labiausiai kibernetinių atakų paveikti sektoriai.

Antrasis darbo skyrius skirtas empirinio tyrimo metodikai aprašyti. Šiame skyriuje pateikiamas tyrimo planas, aprašomas tyrimo metodas, tyrimo imtis ir respondentai bei apribojimai. Detalizuojami tyrimo rezultatų analizei naudojami statistiniai metodai ir įrankiai.

Trečiajame darbo skyriuje pristatomi tyrimo rezultatai ir jų analizė. Rezultatų statistinė analizei atlikti naudojami SPSS ir MS Excel įrankiai. Tyrimo rezultatai pristatomi remiantis aprašomąją statistika - patiekiamos rezultatų dažnių diagramos bei pagrindiniai statistiniai įverčiai. Ryšiui tarp tyrimo konstruktų nustatyti ir hipotezių tikrinimui atliekamos koreliacinė ir tiesinė regresinė analizė, kurių pagrindu pateikiamos išvados ir rekomendacijos.

1. PAGRINDINIAI KIBERNETINĖS RIZIKOS IR JOS VALDYMO TEORINIAI ASPEKTAI

Šiame skyriuje siekiama atskleisti pagrindinius su kibernetinės rizikos ir jos valdymu susijusius aspektus įvardijant kibernetinės rizikos sampratą, kibernetinių incidentų tipus bei kibernetinio saugumo sąvoką. Toliau šiame skyriuje išskiriami kibernetinio saugumo veiksniai ir aprašoma veiklos rezultatų samprata bei kibernetinės rizikos valdymo įtaka įmonių veiklai. Taip pat įvardijami labiausiai kibernetinių atakų veikiami sektoriai ir pateikiama finansinių technologijų (Fintech) sektoriaus Lietuvoje apžvalga.

1.1 Kibernetinės rizikos samprata

Rizika mokslinėje literatūroje yra apibūdinama labai įvairiai. Dažniausiai rizika yra siejama su grėsme, tikimybe įvykti pavojui bei neigiamu poveikiu organizacijai, tačiau rizika gali būti siejama ne tik su neigiamais aspektais, bet ir su sėkme. Sėkmė šiuo atveju dažniausiai siejama su investicine veikla, kuomet remiantis grąžos ir rizikos tiesiogine priklausomybe, prisiėmus didesnį rizikos lygį, įmanoma nebūtinai patirti nuostolių, bet ir uždirbti daugiau nei nerizikavus - gauti didesnę pridėtinę vertę. Šiame darbe rizika yra labiau siejama su neigiama puse, nes grėsmė IT saugai įprastai turi nepalankų poveikį organizacijai, jos klientams ir su ja tiesiogiai susijusios aplinkos subjektams. Bendrai apibūdinant riziką, tai yra nuokrypio nuo laukiamo rezultato galimybė (Norvaišienė, 2005). Rizika yra matas, nurodantis, kokiu mastu subjektui kyla grėsmė dėl galimos aplinkybės arba įvyko, ir paprastai priklauso nuo: neigiamo poveikio, kuris atsirastų, jei įvyktų galima aplinkybė arba įvykis ir įvykio tikimybės (Committee on National Security Systems, 2015).

Rizikos aspektas yra labai svarbus ir bet kokios organizacijos mastu. Šiuolaikiniame pasaulyje įmonės veikloje labai svarbus vaidmuo tenka informacinėms technologijoms, jas taikant galima ne tik pagerinti verslo procesus, optimizuoti resursus, mažinti sąnaudas, pagerinti sprendimų priėmimo valdymą, bet ir pasiekti įmonės užsibrėžtų strateginių tikslų, susijusių su įmonės konkurencingumo didinimu, efektyvesniu įmonės pridėtinės vertės kūrimu (Janeliūnienė & Davidavičienė, 2013). IT naudojimas organizacijoje būtinai turi būti suprantamas ne tik kaip pridėtinės vertės kūrimo įrankis, tačiau turi būti siejamas ir su kylančiomis rizikomis, nes su IT sauga susiję neapibrėžtumai informacinėse ar verslo sistemose gali turėti neigiamų pasekmių įmonei ir jos veiklos tęstinumui (Janeliūnienė & Davidavičienė, IT rizikos identifikavimo proceso analizė, 2013).

IT saugos rizikos sąvoka mokslinėje literatūroje yra įvardinama įvairiai. Su informacine sistema susijusi saugumo rizika – tai rizika, kylanti dėl informacijos ar informacinių sistemų konfidencialumo, vientisumo ar prieinamumo praradimo ir atspindi galimą neigiamą poveikį organizacijos veiklai (įskaitant misiją, funkcijas, įvaizdį ar reputaciją), organizacijos turtui, asmenims, kitoms organizacijoms (Committee on National Security Systems, 2015). IT saugos rizika gali būti apibrėžiama ir kaip tiesiog galima žala organizacijos vertei, dėl netinkamo procesų ir technologijų valdymo (Savić, 2008). IT saugos rizika apima nesugebėjimą reaguoti į saugumo ir privatumo reikalavimus, žmonių klaidas, vidinį sukčiavimą manipuliuojant programine įranga, išorinių įsibrovėlių sukčiavimą, mašinų ir programų senėjimą, patikimumo problemas ar netinkamą valdymą (Savić, 2008). Remiantis Smith ir McKeen (2009) požiūriu dabartinė IT saugos rizika veikianti organizacijas yra kur kas kompleksiškesnė sąvoka. ,,IT saugos rizika keičiasi. IT saugos rizikos incidentai kenkia įmonėms ir už jos ribų. Jie kenkia įmonės reputacijai ir atskleidžia įmonių vadovų trūkumus. Svarbiausia – IT saugos rizika mažina organizacijos konkurencingumą“ (Westerman & Hunter, 2007).

Iškilusi bet kokio tipo IT saugos problema, susijusi su programa, tinklu, nauja sistema, pardavėju ar įsilaužėliu (ar kitos) turi didelį potencialą sukelti pavojų įmonės:

- Prekiniam ženklui;
- Reputacijai;
- Konkurencingumui;
- Finansinei vertei;
- Veiklos efektyvumui ir sėkmei (McKeen & Smith, 2009).

Kibernetinė rizika yra IT rizikos pogrupis. IT saugumas reiškia duomenų ir informacinių sistemų apsaugą nuo neteisėtos prieigos. Tai apima procesų įgyvendinimą, kurie užkerta kelią neskelbtinos įmonės informacijos naudojimui, keitimui ar vagystei. Kibernetinis saugumas apima duomenų apsaugą internete, ypač nuo įsilaužėlių ir kitų kibernetinių nusikaltėlių.

Kibernetinė rizika yra bet kokia rizika, susijusi su finansiniais nuostoliais, veiklos sutrikdymu ar organizacijos reputacijos sugadinimu dėl įvykio, turinčio įtakos organizacijos informacijai ir (arba) informacinėms sistemoms; tai yra rizika atsiradusi dėl informacijos ir ryšių technologijų sukeltų pavojų duomenų ir paslaugų konfidencialumui, prieinamumui ir vientisumui (OECD, 2017).

Konfidencialumo problemų kyla, kai įmonėje esanti privati informacija atskleidžiama trečiosioms šalims, pavyzdžiui, duomenų saugumo pažeidimo atveju; vientisumo problemos yra

susijusios su piktnaudžiavimu sistemomis – sukčiavimu; prieinamumo problemos yra susijusios su verslo sutrikimais (Antoine, 2018).

Daugiau kibernetinės rizikos sampratos apibrėžimų pateikiama lentelėje (žr. **1 lentelė**).

1 lentelė

Kibernetinės rizikos apibrėžimai

Apibrėžimas	Autorius
Pagrįstai nustatoma aplinkybė ar įvykis, galintis turėti neigiamą poveikį ryšių ir informacinių sistemų saugumui.	LR Kibernetinio saugumo įstatymas (2018)
Operacinė rizika informacijos ir technologijų turtui, kurios pasekmės turi įtakos informacijos ar informacinių sistemų konfidencialumui, prieinamumui ar vientisumui.	Cebula, Young (2010)
Rizika patirti finansinius nuostolius, sutrikdyti ar sugadinti organizacijos reputaciją dėl tam tikro jos informacinių technologijų sistemos gedimo.	IRM (2018)
Rizika, susijusi su kenkėjiškas elektroniniais įvykiais, sukeliančiais trikdžius verslui ir piniginius nuostolius. Kibernetinė rizika apima visas rizikas, susijusias su veikla internete, pvz., asmens duomenų saugojimas internete arba internetinių sandorius, dėl kurių gali atsirasti žala reputacijai, finansinių nuostolių, gyvybės arba verslo sutrikdymas.	NAIC, 2018.
Verslo rizika susijusi su IT naudojimu, nuosavybe, veikimu, įtraukimu ir įtaka verslo veikloje. Ją sudaro su IT susiję įvykiai, kurie gali turėti įtakos verslui.	ISACA, (2009)

Šaltinis: sudaryta autoriaus, remiantis lentelėje pateiktais šaltiniais

Apibendrinus kibernetinės rizikos apibrėžimai gali būti išskaidomi pagal:

- Kibernetinės rizikos šaltinius;
- Kibernetinės rizikos objektus;
- Kibernetinės rizikos poveikį;
- Sudėtiniai, sudaryti iš rizikos šaltinių, objektų bei poveikio (Strupczewski, 2021).

Remiantis Strupczewski (2021) atlikta kibernetinės rizikos apibrėžimų analize, geriausiai kibernetinę riziką apibūdina šis apibrėžimas: „kibernetinė rizika yra operacinė rizika susijusi su veiklos vykdymu elektroninėje erdvėje, kuri yra pavojinga informacijos ir technologiniam turtui

bei informacinių ir ryšių technologijų (IRT) šaltiniams bei gali padaryti materialinę žalą organizacijos materialiajam ir nematerialiajam turtui, nutraukti veiklą ar pakenkti reputacijai. Kibernetinė rizikos sąvoka taip pat apima fizines grėsmes organizacijos informacinių ir ryšių technologijų šaltiniams.“

Kibernetinės rizikos yra dinamiškos dėl nuolatinių IT naujovių, intensyvėjančio pasaulinio ryšio ir didėjančio įsilaužėlių sumanumo (Sheehan, Murphy, Mullins, & Ryan, 2019). Visai tai kibernetinę riziką paverčia kompleksišku sudėtingu reiškiniu.

1.2 Kibernetinių incidentų klasifikacija

Svarbu paminėti, jog kibernetinė rizika egzistuoja visada, nepaisant to, ar ji aptinkama ir atpažįstama organizacijos, ar ne. IT saugos pažeidimai sukelia verslo procesų sutrikimus, (kritinį) infrastruktūros sutrikdymą ir fizinę žalą nei tik organizacijos nuosavybei, bet ir žmonėms.

Kibernetinę riziką gali sukelti stichinės nelaimės arba žmogus. Kibernetiniai incidentai gali įvykti dėl žmogaus klaidos, kibernetinio nusikalstamumo, kibernetinio karo arba kibernetinio terorizmo (Eling & Schnell, 2017). Kibernetinė rizika gali būti ir nesusijusi su tiesioginėmis kibernetinėmis atakomis, pavyzdžiui, programinės įrangos atnaujinimai arba stichinės nelaimės gali sukelti pavojų verslo procesams be jokių kibernetinio sukčiavimo priemonių (Antoine, 2018). Šiuolaikiniame pasaulyje kai dauguma organizacijų yra priklausomos nuo IT, o informacija bei duomenys yra galios priemonė, dažniausiai kibernetinės rizikos pavojus visgi kyla dėl kibernetinių incidentų.

Remiantis LR Kibernetinio saugumo įstatymu (2018), kibernetinis incidentas yra įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.

Pagal Setianingsih, Pulungan, Putra, Wibowo, ir Syarip (2021) kibernetiniai incidentai yra išskiriami į tris kategorijas:

- Aktyvios atakos;
- Pasyvios atakos;
- Kibernetiniai karai.

Aktyvios kibernetinės atakos/incidentai reiškia veiklą, kuri pažeidžia informacines sistemas, įskaitant žvalgybos atakas, prieigos atakas, elektroninius nusikaltimus, kibernetinį šnipinėjimą, kibernetinį terorizmą, kenkėjiškas ir nepiktybines atakas prieš mobiliuosius „ad hoc“ tinklus ir belaidžius jutiklių tinklus.

Pasyvios atakos nėra susijusios su sistemomis, bet labiau fokusuojasi į svarbios informacijos išsaugojimą tolesniam panaudojimui (Setianingsih, Pulungan, Putra, Wibowo, & Syarip, 2021).

Kibernetinis kartas tai – valstybės atakos siekiant sutrikdyti ar padaryti žalą kitai valstybei prasiskverbiant į kitos valstybės kompiuterius ar tinklus (Clarke & Knake, 2014).

Pagrindiniai kibernetinių incidentų tipai pateikti lentelėje (žr. **2 lentelė**).

2 lentelė

Kibernetinių incidentų tipai

Kibernetinio incidento tipas	**Aprašymas**
Duomenų konfidencialumo pažeidimas	1. Įvykiai, susiję su organizacijos konfidencialiais duomenimis (pvz., finansiniais duomenimis, komercinėmis paslaptimis, intelektine nuosavybe); 2. Įvykiai, susiję su trečiųjų šalių konfidencialiais duomenimis (klientų asmenine informacija)
Sistemos gedimas, problema	1. Įmonės sistemos gedimas; 2. Sistema, paveikta kenkėjiškų programų; 3. Tinklo ryšio sutrikimas; 4. Netyčinis trečiųjų šalių sistemos sutrikimas; 5. Išorinės skaitmeninės infrastruktūros sutrikdymas.
Duomenų prieinamumas	1. Įmonės ar trečiųjų šalių duomenų panaikinimas arba sugadinimas dėl programinės įrangos klaidos; 2. Įmonės arba trečiųjų šalių duomenų šifravimas dėl išpirkos išpuolių.

Kenkėjiška veikla	1. Piktnaudžiavimas sistema; 2. Kibernetinis sukčiavimas/kibernetinė vagystė (socialinė inžinerija)

Šaltinis*:* sudaryta autoriaus, remiantis OECD (2017).

Duomenų konfidencialumo pažeidimai yra vieni iš dažniausių kibernetinių incidentų tipų. Jie gali įvykti dėl žmogaus klaidų ar kenkėjiškų atakų, kurių metu atsiranda rizika pažeisti organizacijos ar trečiųjų šalių konfidencialius duomenis.

Antrasis kibernetinių incidentų tipas lentelėje yra sistemos gedimas ar problema, kurios smulkiau išskiriamos į 5 smulkesnius tipus:

- Įmonės sistemos gedimas yra sistemos klaidos, sistemos nereagavimas į įvestis dėl kurių sistema nustoja veikti.
- Sistema, paveikta kenkėjiškų programų - įtariamas įsibrovimas į sistemą dėl kenkėjiškų programų aptikimo arba nenormalaus sistemos ir programinės įrangos elgesio.
- Tinklo ryšio sutrikimas atsiranda, kai sistemos negali susisiekti internetu ar kitu skaitmeniniu tinklu.
- Netyčinis trečiųjų šalių sistemos sutrikimas: atvejai kai įvyksta įsilaužimas į organizacijos sistemas ar tinklus tam, kad pakenktų trečiajai šaliai. Organizacijos, kurios tinklai ar sistemos buvo panaudotos kenkėjiškos programos perdavimui, gali patirti trečiosios šalies atsakomybės reikalavimus iš šalies, kuri nukentėjo.
- Išorinės skaitmeninės infrastruktūros sutrikdymas - tai reiškia įmonės verslo sutrikimą, atsirandantį dėl trečiosios šalies teikiamų informacinių technologijų paslaugų paskirstymo (pvz. debesų technologijos paslaugos) (OECD, 2017).

Trečiasis kibernetinių incidentų tipas yra duomenų prieinamumas. Tai yra įmonės ar trečiųjų šalių duomenų panaikinimas arba sugadinimas dėl programinės įrangos klaidos, kuris gali įvykti dėl žmonių klaidos ar kenkėjiškos atakos (OECD, 2017). Įmonės arba trečiųjų šalių duomenų šifravimas dėl išpirkos vyksta kai užpuolikai panaudoja kompiuterines programas (ang. „ransomware“), kurios blokuoja vartotojų prisijungimą prie įvairių sistemų ar duomenų iki tol kol nebus išpildytos išpirkos sąlygos (OECD, 2017).

Ketvirtasis tipas yra įvardijamas kaip kenkėjiškai veikla, kuri išskiriama į kelis smulkesnius tipus:

- Piktnaudžiavimas sistemomis - piktnaudžiavimas skaitmeninėmis sistemomis siekiant platinti šmeižikišką ar gėdingą informaciją (OECD, 2017). Tokie incidentai gali sukelti didelę reputacinę žalą.
- Kibernetinis sukčiavimas/kibernetinė vagystė įvardijama kaip įsilaužimas į įmonės tinklus ir finansinius įgaliojimų naudojimas neteisėtam pervedimui atlikti (OECD, 2017). Tokio incidento metu galimi dideli finansiniai nuostoliai.

Kibernetiniam sukčiavimui ar vagystėms įvykdyti dažnai yra naudojama ir socialinė inžinerija. Socialinės inžinerijos terminas siejamas su informacijos saugumo pažeidimais pasinaudojus žmogiškuoju faktoriumi. Socialinė inžinerija yra apibūdinama kaip ataka kai naudojantis ne technologijomis, bet manipuliuojant ir klaidinant žmones yra išgaunama naudinga informacija (Shimonski, 2016). Šis metodas gana dažnai naudojamas, nes žmonės (atvirkščiai, nei sistemos ir įrenginiai) socialiniame kontekste gali būti paveikti įvairių psichologinių priemonių.

Apibendrinus, šie pagrindiniai kibernetinių incidentų tipai turi skirtinga poveikį: verslo (duomenų prieinamumo) sutrikimai trukdo įmonėms sklandžiai vykdyti savo veiklą, dėl to negaunamos pajamos; sukčiavimo (informacijos saugos vientisumo) incidentai sukelia tiesioginius finansinius nuostolius, o duomenų saugumo (duomenų konfidencialumo) pažeidimo pasekmės pasireiškia po ilgesnio laikotarpio dėl reputacijos poveikio ir bylinėjimosi išlaidų (Antoine, 2018). Konfidencialumo praradimo incidentai gali turėti rimtų padarinių klientų pasitikėjimui verslu; verslo sutrikimo incidentai dažniausia turi tiesioginių, bet kur kas trumpesnių padarinių nei sukčiavimas ar duomenų pažeidimai.

1.3 Kibernetinis saugumas ir pagrindiniai jo komponentai

Išsiaiškinus kibernetinė rizikos sampratą bei kibernetinių incidentų klasifikaciją, svarbu apsibrėžti ir kibernetinio saugumo sąvoka bei pagrindinius komponentus.

Pagrindinis kibernetinio saugumo dėmesys yra turto (įskaitant žmones), duomenų, sistemų ir organizacijos apsauga remiantis naujomis informacinėmis technologijom bei vyriausybės reglamentais. Kibernetinis saugumas taip pat apima ir rizikos analizę, įskaitant grėsmes, pažeidžiamumą ir sukčiavimą, kad būtų galima numatyti įvairius kibernetinių atakų scenarijus (Setianingsih, Pulungan, Putra, Wibowo, & Syarip, 2021).

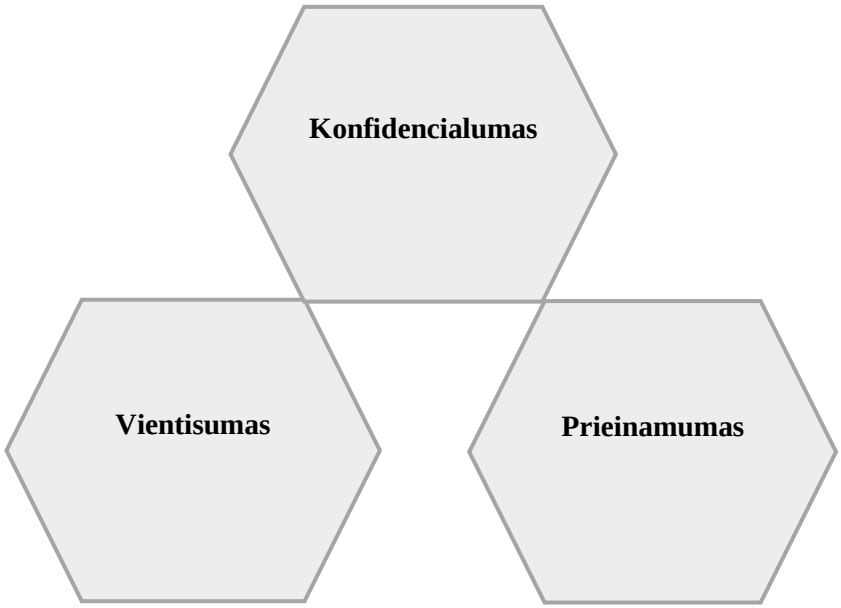
Remiantis LR Kibernetinio saugumo įstatymu (2018), kibernetinis saugumas – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos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

Nacionalinis kibernetinio saugumo centras (2022), kibernetinį saugumą įvardina kaip veiksmus, kurių imamasi norint apsaugoti kibernetinę aplinką ir užtikrinti informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumą, vientisumą bei konfidencialumą. Kibernetinio saugumo sąvoka labiau apima įvairių priemonių visumą tam, kad būtų galima apsaugoti informacines sistemas bei jose tvarkomus duomenis nuo trikdžių, neteisėtos veiklos ir atakų.

Kibernetinis saugumas yra užtikrinamas 3 pagrindiniais aspektais, kurie pavaizduoti paveiksle (žr. **1 paveikslas**).

1 paveikslas

Kibernetinio saugumo užtikrinimo aspektai



Šaltinis: sudaryta autoriaus, remiantis Nacionaliniu Kibernetiniu saugumo centru (2022).

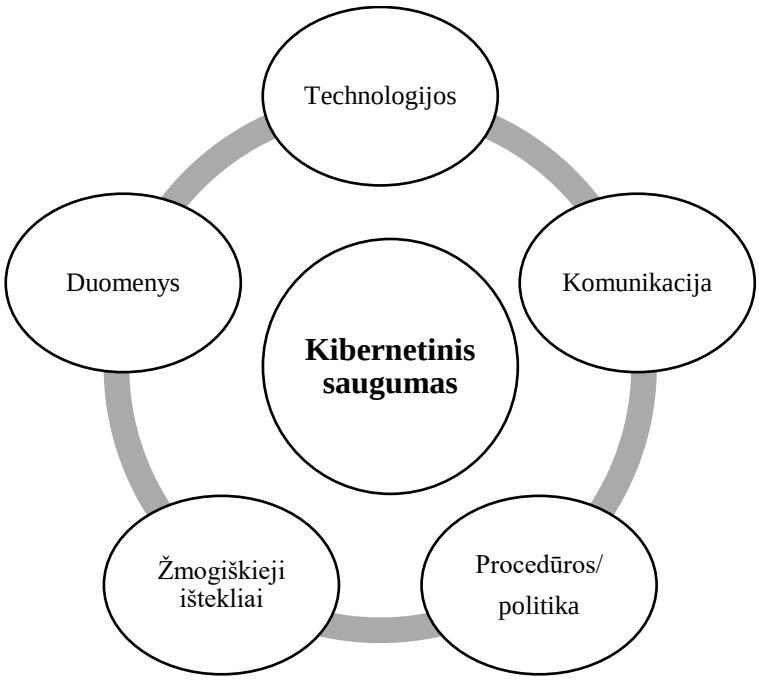
Pagal Nacionalinį kibernetinio saugumo centrą (2022) informacijos konfidencialumas, vientisumas ir prieinamumas apibūdinami taip:

- Konfidencialumas yra konfidencialios informacijos pasiekiamumas, tik tiems asmenims, kuriems tai yra reikalinga - bet kokia įmonės, klientų ar verslo partnerių informacija yra pasiekiama tik įgaliotiems asmenims, kuriems yra būtina žinoti, ir jiems suteikta tokia prieiga.
- Vientisumas – užtikrinimas, kad informacija ir duomenys yra teisingi, nėra atsitiktinai ar neteisėtai pakeisti ir sunaikinti. Duomenys dažniausiai suklastojami dėl kenkimo programinės įrangos ar neteisėto užvaldymo, techninės ar programinės įrangos gedimo.
- Prieinamumas – užtikrinimas, kad visada yra prieiga prie tam tikros informacijos, duomenų bazės ar kitų elektroninių paslaugų. Įmonėje tai galėtų būti nuolatinės svetainės ar duomenų bazės prieigos užtikrinimas. Sutrikus veiklai ir nesant galimybės pasiekti reikiamą informaciją, net ir trumpą laiką, įmonė gali būti priversta laikinai nutraukti savo veiklą ir prarasti pajamas, sukelti klientų nepasitenkinimą bei pakenkti savo reputacijai.

Informacijos konfidencialumui, vientisumui ir prieinamumui užtikrinti padeda kibernetinio saugumo komponentai atvaizduoti paveiksle (žr. **2 paveikslas**).

2 paveikslas

Kibernetinio saugumo komponentai



Šaltinis: sudaryta autoriaus, remiantis Setianingsih, Pulungan, Putra, Wibowo ir Syarip (2021).

Setianingsih, Pulungan, Putra, Wibowo ir Syarip (2019) išskiria 5 pagrindinius kibernetinio saugumo komponentus, kurie yra:

1. **Duomenys**: informacija perduodama per tinklą.
2. **Technologijos**: programinė įranga apima programų paketus, operacines sistemas, įskaitant platformas, skirtas valdyti prietaisus ir valdymą, kurie yra pažeidžiami atakų metu; techninę įrangą apima fizines įrangos dalis ir kitus išorinius (periferinus) įrenginius.
3. **Procedūros/politikos**: nacionalinės ir tarptautinės taisyklės, kurių reikia laikytis.
4. **Žmogiškieji ištekliai:** darbuotojai, atsakingi už sklandų sistemos, įrenginių veikimą, jų įgūdžiai.
5. **Komunikacija:** sąveika tarp įrenginių, tinklo ir žmogaus-mašinos sąsajos (angl. *Interface*).

Atsargumo priemonės, kurios turi būti naudojamos kaip prevencija kibernetinėms atakoms, gali būti: užšifruotų duomenų naudojimas (1); programinės ir techninės įrangos įsigijimas iš įvairių tiekėjų, saugus programinės įrangos atnaujinimas, atitinkantis kokybės užtikrinimą, periodinė techninės įrangos priežiūra ir patikra (2); reglamentuotų reikalavimų atitikimas (3); tinkami darbuotojų mokymai ir reguliarus kompetencijos plėtimas (4); komunikacijos autentiškumo užtikrinimas (5) (Setianingsih, Pulungan, Putra, Wibowo, & Syarip, 2021).

Kibernetinis saugumas apima vidinius teisės aktus, organizacinius procesus ir technines priemones, leidžiančias išvengti, aptikti ir reaguoti į kibernetinius incidentus, įvertinti rizikas (Nacionalinis kibernetinio saugumo centras, 2022). Kibernetinį saugumas yra gana kompleksiškas, nes susideda iš gana plačių komponentų, kurių pagrindu taikant atitinkamas priemones siekiama apsaugoti informacines sistemas ir užtikrinti informacijos saugumą nuo galimo neigiamo poveikio.

Bendrai rizikos valdymas gali būti įvardijamas kaip procesas, kuris apima rizikos nustatymą, rizikos įvertinimą bei veiksmų priėmimą, kurių pagrindu siekiamą sumažinti riziką iki priimtino lygio (Stoneburner, Goguen, & Feringa, 2002). CNSS (2015) rizikos valdymą įvardija kaip programą ir pagalbinius procesus, skirtus valdyti informacijos saugumo riziką organizacijos operacijoms (įskaitant misiją, funkcijas, įvaizdį, reputaciją), organizacinį turtą, asmenis, kitas organizacijas ir tautą, ir apima: (i) su rizika susijusios veiklos konteksto nustatymą; ii) rizikos vertinimą; iii) reagavimą į riziką, po jos nustatymo; ir iv) rizikos stebėjimą.

Pagal Janeliūnienę ir Davidavičienč (2013), ,,rizikos valdymas yra procesas, kai rizikos identifikuojamos, įvertinamos ir imamasi priemonių kaip sumažinti rizikas iki priimtino lygio“.

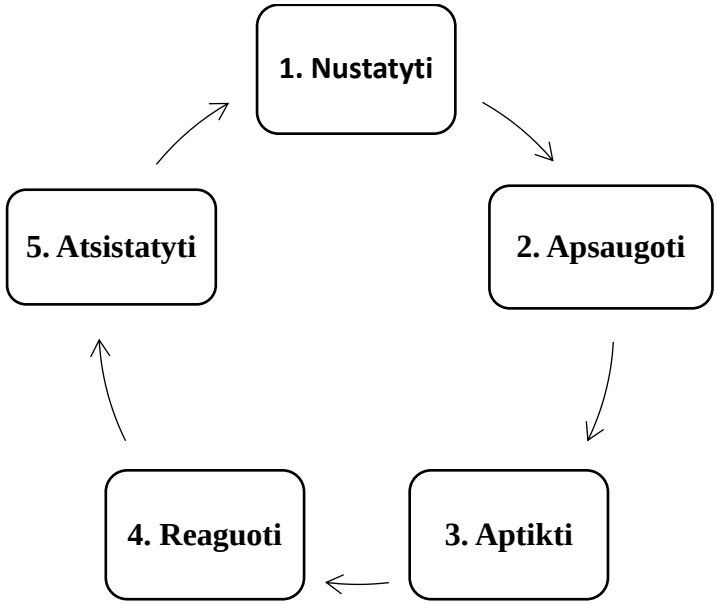
Pagrindiniai kibernetinės rizikos valdymo tikslai:

1. Apsaugoti IT sistemas, kurios susijusios su organizacijos informacijos saugojimu, apdorojimu ir perdavimu;
2. Sudaryti galimybę vadovams priimti savalaikius rizikos valdymo sprendimus;
3. Pasiruošti tinkamai reaguoti į incidentus ir sumažinti galimus neigiamus padarinius (Stoneburner, Goguen, & Feringa, 2002).

Kibernetinio saugumo sistema ir jos pagrindinės funkcijos pavaizduotos paveiksle (žr. ***3*** **paveikslas**).

3 paveikslas

Kibernetinio saugumo sistema



Šaltinis: sudaryta autoriaus, remiantis Wilson (2019).

Kibernetinio saugumo sistema turi penkis pagrindinius etapus (Wilson, 2019):

1. **Nustatyti.** Norėdami vykdyti veiksmingą kibernetinio saugumo sistemą, vadovai pirmiausia turi nustatyti komponentus (tam, kad galėtų teisingai paskirstyti laiką ir išteklius):
    - vidines ir išorines kibernetinio saugumo grėsmes ir riziką;

- vidinius ir išorinius užpuolikus;
- svarbiausią turtą, kurį reikia apsaugoti nuo kibernetinio incidento (klientų ir darbuotojų duomenys, kritinės IT ir operacinės sistemos);
- suinteresuotus subjektus, atsakingus už veiksmingos kibernetinio saugumo programos diegimą;
- procesus, sistemas ir išteklius, kurie turėtų būti įdiegti ir vykdyti kibernetinio saugumo programą.

2. **Apsaugoti.** Po nustatymo etapo vadovai turi imtis veiksmų, kad tinkamai apsaugotų organizaciją. Šio etapo metu svarbu įsivertinti galimybes:
   - Ar vadovybė turi pakankamą apsaugą, kad galėtų kontroliuoti prieigą prie fizinio ir skaitmeninio turto ir susijusių įrenginių? Ar ribojamas įgaliotų naudotojų procesų ir įrenginių prieigos lygis, atitinka su kiekvienu turtu susijusios rizikos lygį?
   - Ar vadovybė turi tinkamą saugumo politiką, procesus ir procedūras, kurių nuosekliai laikomasi?
3. **Aptikti**. Trečiajame etape vadovai turėtų būti susipažinę su terminu "anomali veikla", kuris apibūdina sistemų ar žmonių, kurie nepatenka į įprastą elgesį, veiklą. Anomalijos yra saugumo veiksniai, kuriuos vadovybė turėtų stebėti.
4. **Reaguoti.** Saugumo pažeidimai gali būti neišvengiami net ir taikant geras saugumo priemones. Kai kibernetiniai incidentai įvyksta, vadovai turi mokėti veiksmingai reaguoti. Efektyvi reakcija gali padėti užkirsti kelią incidento plėtrai ir didesniam neigiamam poveikiui. Reakciją tobulinti gali padėti nuolatinis mokymasis ir kompetencijos plėtimas.
5. **Atsistatyti**. Paskutinis etapas yra atsistatymas po incidento. Vadovai turėtų įsitikinti ar atsistatymo pajėgumai yra tinkami, kad būtų galima:
   - atkurti sistemas ar turtą, kurį paveikė kibernetinis incidentas (atsarginės duomenų programos, tinklai, IT ir operacinės sistemos);

- koordinuoti atsistatymo veiklą su vidaus ir išorės suinteresuotais subjektais (interneto paslaugų tiekėjai, atakuojančių sistemų savininkai).

Galima daryti išvadą, jog kibernetinio saugumo sistemos funkcijos yra labai tarpusavyje susijusios, o pats kibernetinio saugumo procesas turėtų būti įgyvendinamas nuolat. Kibernetinio saugumo valdymas yra daugiasluoksnė koncepcija, teigianti, kad kibernetiniai įvykiai kenkia tiek įmonei, tiek jos klientams (McKeen & Smith, 2009).

Remiantis Jevsejev (2020), vienas iš rizikos valdymo užtikrinimo metodų yra rizikos vertinimas. Yra daug metodų, kurie atitinka kibernetinio saugumo rizikos vertinimo poreikius, tačiau skirtingoms organizacijoms metodai gali būti adaptuojami pagal organizacijos poreikius, atsižvelgiant į organizacijos priklausomybę nuo informacijos. Siekiant kokybiško kibernetinio saugumo užtikrinimo, rekomenduotina kreiptis i specialistus, tačiau įmonės ir pačios gali atlikti rizikos valdymo bei identifikavimo funkcijas.

Rizikų vertinimo metodologijos ir gerosios kibernetinio ir informacinio saugumo valdymo praktikos yra pateikiamos įvairiuose tarptautiniuose standartuose (pvz. ISO, NIST). ISO/IEC 27001 yra tarptautinis informacijos saugos valdymo sistemų (ISVS) standartas. Šiame standarte pateikiama aiški ir išsami specifikacija, skirta organizacijos informacijai apsaugoti ir išlaikyti pagal konfidencialumo, vientisumo ir prieinamumo principus. Standartas siūlo geruųjų praktikų kontrolės priemonių rinkinį, kuris gali būti taikomas organizacijai, atsižvelgiant į riziką, su kuria susiduriama. Standartą taip pat galima taikyti integruojant su keliais kitais standartais, įskaitant NIST CSF (kibernetinio saugumo sistemą) ir NIST RMF (rizikos valdymo sistemą). NIST CSF (Nacionalinis standartų ir technologijų instituto) kibernetinio saugumo sistema yra skirta valdyti ir sumažinti organizacijų kibernetinio saugumo riziką, remiantis esamais standartais, gairėmis ir gerosiomis praktikomis. NIST standartas žymus penkiais reagavimo į incidentus žingsniais - identifikuoti, apsaugoti, aptikti, reaguoti ir atkurti. Pastovus šių standartų diegimas padeda apsisaugoti nuo vidinių ir išorinių saugumo grėsmių. Mažesnėms įmonėms šie standartai gali būti gana kompleksiški, o jų įgyvendinimas reikalauti daug kaštų, tačiau tai yra naudingi šaltiniai, padedantys verslui įvertinti pasiruošimą reaguoti į kibernetinius incidentus (Nacionalinis kibernetinio saugumo centras, 2022).

Rizikos nustatymo procese turėtų dalyvauti visi asmenys, dirbantys su IT - aukščiausio ir vidutinio lygmens vadovai, IT, informacijos saugumo ir kiti specialistai (Janeliūnienė & Davidavičienė, IT rizikos indetifikavimo proceso analizė, 2013). Rizikų vertinimas turi būti suprantamas kaip ne vienkartinis veiksmas, o nuolat kartojamas verslo procesas (Nacionalinis

kibernetinio saugumo centras, 2022). Pagal kibernetinio saugumo vadovą (2022), rekomenduojama periodiškai (ne rečiau kaip kartą per dvejus metus) peržiūrėti ir iš naujo atlikti rizikos vertinimą. Jeigu diegiamos naujos IT sistemos, įrenginiai arba keičiami verslo procesai, prieš tai atliekant - įmonės turėtų atlikti ir kibernetinių rizikų vertinimą.

1.4 Kibernetinio saugumo veiksniai

Kibernetinio saugumo pasirengimas priklauso nuo anksčiau išvardintų komponentų, tačiau taip pat galima išskirti ir veiksnius, kurie turi įtakos įmonių kibernetinio saugumo pasirengimui.

Mokslinių šaltiniuose yra įvardijama IT infrastruktūros įtaka organizacijų kibernetiniam saugumui ir pasirengimui kovoti su kibernetinėmis atakomis. Hsu ir kt (2012) ir Angst ir kt. (2016) įvardina, jog kibernetiniam saugumui įtakos turi IT prieinamumas ir panaudojimas kibernetinėms rizikoms valdyti organizacijoje. IT infrastruktūros prieinamumas ir panaudojimas sumažina kibernetinių incidentų skaičių organizacijoje ir informacijos saugumo pažeidžiamumą (Kong, Kim, & Kim, 2012). Chang and Ho (2006) nustatė teigiamą ryšį tarp IT pajėgumų ir IT saugos valdymo įgyvendinimo organizacijose, dėl IT sistemų ir išteklių panaudojimo saugos įspėjimų stebėjimui ir kontrolei.

Moksliniuose šaltiniuose aukščiausios vadovybės palaikymas įvardijamas kaip vienas iš esminių kibernetinio saugumo elementų (Kraemer, Carayon, & Clem, 2009) (Soomro, Hussain Shah, & Ahmed, 2016). Aukščiausioji vadovybė gali paveikti darbuotojų elgesį organizacijos saugumo politikos ir strategijų atžvilgiu, tačiau tokia įtaka reikalauja aukščiausios vadovybės įsipareigojimo ir įsitraukimo. Vertinant aukščiausios vadovybės palaikymo įtaką IT saugos rizikos valdymui, Hsu ir kt. (2012) nustatė, kad aukščiausios vadovybės įsitraukimas į IT saugumo valdymo procesą skatina kibernetinio saugumo efektyvumą organizacijoje. Kankanhalli ir kt. (2003) teigia, kad aukščiausioji vadovybė gali palaikyti kibernetinį saugumą asmeniškai dalyvaudama saugumo politikos, gairių formavimo procese. Taip pat svarbus aukščiausios vadovybės įsitraukimas formuojant organizacijos viziją, strategiją, tikslus ir standartus atsižvelgti į IT saugumą (Liang, Saraf, Hu, & Xue, 2007).

Organizaciniai įgūdžiai, tiksliau, organizacijos darbuotojų įgūdžiai daugelyje mokslinių šaltinių išryškinami kaip svarbus veiksnys siekiant palaikyti kibernetinį saugumą organizacijose. Wixom ir Watson (2001) įvardina, kad svarbu turėti darbuotojų, turinčių stiprių techninių įgūdžių, kad būtų galima geriau išspręsti saugumo problemas. Pagal D'Arcy ir kt. (2014), nuolatinis darbuotojų mokymas ir kompetencijos kėlimas padeda kovoti su kibernetinėmis atakomis ir taip stiprina kibernetinį saugumą.

Remiantis literatūros šaltiniais, kibernetiniam saugumui įtakos turi ir organizacijos kultūra. Organizacijos kultūra formuoja darbuotojų elgesį ir vertybes saugumo atžvilgiu. Dalijimasis žiniomis ir bendradarbiavimas daro įtaką organizacijos saugumo valdymui, o tai gali teigiamai paveikti organizacijos rezultatus (Tang, Li, & Zhang, 2016). Gopal ir Gosain (2010) pabrėžia bendradarbiavimo ir organizacinės kultūros kūrimo svarbą skatinant efektyvesnio IT saugos rizikos valdymo. Saugumo taisyklių suvokimas ir laikymasis yra irgi svarbus siekiant gerinti organizacijos kibernetinį pasirengimą (Iivari & Huisman, 2007).

Organizacijos pasirengimui kovoti su kibernetinėmis atakomis taip pat turi įtakos bendradarbiavimas su konkurentais saugumo klausimais. Nemažai tyrimų yra vertinamas konkurentų bendradarbiavimas kibernetinio saugumo kontekste ir daroma išvada, kad organizacijos gali geriau numatyti atakas ir su jomis kovoti, kai konkurentai nuolat informuoja apie naujus incidentus (Kianpour, Øverby, James Kowalski, & Frantz, 2019) (Seppänen, 2020). Pasak Bouncken ir Fredrich (2016), organizacijos gali greičiau spręsti problemas, kai naudojasi žiniomis, gautomis iš konkurentų. Dalijimasis naujomis idėjomis ir įgūdžiais tarp konkurentų gali pagerinti organizacijos pasirengimą reaguoti į kibernetines atakas.

Dar vienas svarbus veiksnys - bendradarbiavimas su partneriais, kuris yra esminis veiksnys siekiant laiku sustabdyti kibernetinį incidentą dėl atviro bendravimo ir laiku užtikrintos atskaitomybės partneriams saugumo klausimais (Krishnan, Martin, & G. Noorderhaven., 2006). Atlikus literatūros analizę, pastebėtas ryšys tarp santykių su verslo partneriais ir pasirengimu kovojant su kibernetinėmis atakomis, kuris pagrįstas abipusiu pasitikėjimu ir bendradarbiavimu.

Valstybės reguliavimas įvardijamas kaip dar vienas iš veiksnių, kuris padeda organizacijoms išlaikyti informacijos saugumą (Wall, Benjamin Lowry, & B. Barlow, 2015). Valstybė gali imtis įvairių veiksmų, kad reguliuotų organizacijų kibernetinį saugumą. Pagal Zhu ir Kraemeris (2005) svarbus valstybės vaidmuo reguliuojant organizacijų kibernetinį saugumą pasireškia per atitinkamų įstatymų kūrimą ir internetinių sandorių apsaugą, paverčiant internetą patikima verslo platforma. Valstybės reglamentai ir sankcijos, kurie verčia organizacijas geriau vykdyti taisykles ir užtikrinti atitinkamą saugumo lygį, lemia didesnį kibernetinio saugumo pasirengimą (Wall, Benjamin Lowry, & B. Barlow, 2015).

Valstybės parama yra svarbi užtikrinant organizacijų kibernetinį saugumą. Valstybė gali įvairiai palaikyti organizacijų kibernetinį saugumą įgyvendinat įvairias kibernetinio saugumo programas (Knapp, E. Marshall, Rainer Jr, & W. Morrow., 2006). Valstybė turi būti atsakinga už organizacijų informavimą apie naujausias kibernetines atakas, kad būtų galima imtis atitinkamų atsakomųjų veiksmų.

Pramonės standartų laikymasis įvardijamas kaip svarbus veiksnys palaikant organizacijų kibernetinį saugumą (Knowles, Prince, Hutchison, Ferdinand Pagna Disso, & Jones, 2015). Dažnai naudojami šie tarptautinės institucijų standartai, kurie padeda organizacijoms palaikyti kibernetinį saugumą, vadovaujantis gairėmis priimant sprendimus:

- Nacionalinio standartų ir technologijų instituto (NIST) gerosios praktikos;
- Tarptautinės standartų organizacijos (ISO) saugumo gairės;
- Amerikos Nacionalinio standartų instituto (ANSI) taisyklės.

Visus anksčiau įvardintus veiksnius, galima susikarstyti į grupes, pagal kontekstą (žr. **3 lentelė**).

3 lentelė

Kibernetinio saugumo veiksnių grupės

Veiksnių grupė	**Aprašymas**	**Veiksniai**
Technologinis kontekstas	Technologiniai veiksniai (IT ištekliai, sistemos), kurie turi įtakos kibernetiniam saugumui	• IT infrastruktūra; • IT galimybės; • IT investicijos; • Ištekliai IT infrastruktūrai valdyti.
Organizacinis kontekstas	Vidiniai organizacijos veiksniai, kurie turi įtakos kibernetiniam saugumui	• Aukščiausios vadovybės palaikymas; • Darbuotojų įgūdžiai; • Organizacijos kultūra.
Aplinkos kontekstas	Išoriniai organizacijos veiksniai, kurie turi įtakos kibernetiniam saugumui	• Bendradarbiavimas su konkurentais; • Santykiai su partneriais; • Valstybės reguliavimas ir parama; • Pramonės šakos standartai.

Šaltinis: sudaryta autoriaus, remiantis (Hasan, Ali, & Kurnia, 2021).

Technologinės priemonės iš esmės yra organizacijos IT infrastuktūra. Tai susideda ne tik iš IT infrastruktūros ir IT specialistų, reikalingų kibernetinio saugumo valdymui. Taip pat svarbu kaip organizacija išnaudoja IT išteklius, pažangias IT priemones bei metodus kibernetiniam saugumui valdyti.

Prie organizacinių kibernetinio saugumo priemonių priskiriama – aukščiausiosios vadovybės palaikymas, organizacijos darbuotojų įgūdžiai ir kultūra. Aukščiausios vadovybės palaikymas yra vienas iš svarbiausių veiksnių. Jei organizacijoje kibernetinis saugumas yra strategiškai svarbus, ir vadovybė skatina kibernetinio saugumo iniciatyvas bei kuria ir laikosi kibernetinio saugumo politikų ir gairių, neabejotinai tai gerina kibernetinio saugumo pasirengimą. Be to yra svarbi organizacijos kultūra ir darbuotojų įgūdžiai. Svarbu ne tik skatinti bendradarbiavimą ir taisyklių laikymąsi kibernetinio saugumo tema organizacijoje bet ir suteikti reikiamus išteklius darbuotojų mokymams ir kompetencijos augimui.

Aplinkos priemones sudaro organizaciją veikianti aplinka: santykiai su konkurentais, bendradarbiavimas su partneriais, valstybės reguliavimas ir parama bei pramonės šakos standartai. Dalijimasis informacija su konkurentais kibernetinių incidentų tema ir atviras bendradarbiavimas su partneriais padeda mokytis iš klaidų ir taikyti gerąsias praktikas. Valstybės reguliavimas ir parama bei pramonės šakos standartai yra irgi labai svarbios kibernetinio saugumo priemonės. Jų laikymasis padeda mažinti kibernetinių incidentų skaičių ir/ar geriau atsilaikyti kibernetinių išpuolių metu bei atsistatyti po jų.

1.5 Kibernetinės rizikos valdymo svarba įmonės veiklai ir rezultatams

Organizacijos sėkmingai veikla ir rezultatams pasiekti esminiu aspektu tampa ir kibernetinis saugumas, kuris tampa neatsiejama verslo gyvybingumo ir plėtros dalimi (Nacionalinis kibernetinio saugumo centras, 2022). Kibernetinio incidento padariniai įmonėms gali būti labai dideli, gali sutrikdyti verslo pranašumą ar tęstinumą. Įvykus kibernetinei atakai ne tik paralyžiuojama įstaigos ar organizacijos veikla, prarandami intelektiniai ir asmeniniai duomenys, bet ir suduodamas stiprus smūgis reputacijai.

„Statistikos departamento skaičiavimais, 2021 m. 16 proc. įmonių yra turėjusios problemų dėl e. saugos incidentų. Didžiosios įmonės kibernetinių atakų patiria gerokai dažniau – 32,9 proc. Tarp vidutinių įmonių tokių būta 22,8 proc., tarp smulkiųjų – 13,9 proc. Nors draudimo bendrovės siūlo apdrausti verslą nuo e. saugos incidentų, tik 5,2 proc. visų įmonių turi tokį draudimą“ (Lietuvos statistikos departamentas, 2022). Nuostoliai įvykus kibernetiniam incidentui reikalauja didesnių išlaidų nei investicijos į duomenų saugumą, tačiau verslas ne visuomet tinkamai įvertina kibernetines grėsmes.

Lietuvos statistikos departamento skelbiami duomenys rodo, kad ,,kuo mažesnė įmonė, tuo mažiau dėmesio ji skiria saugumo sistemoms internetinėje erdvėje diegti. Pavyzdžiui, šiemet visas tyrime įvardytas saugumo priemones 100 proc. naudojusios 250 ir daugiau darbuotojų turinčios įmonės. Tačiau 50–249 darbuotojus turinčiųjų grupėje šis skaičius siekė 96,4 proc. O mažiausių įmonių, turinčių 10–49 darbuotojus, grupėje visas tirtas saugumo priemones internete naudojo 85,9 proc. “ (Lietuvos statistikos departamentas, 2022).

Remiantis Nacionaliniu kibernetinio saugumo centru (2022), klaida yra galvoti, kad maža įmonė niekada netaps atakos auka ar kad ji paprasčiausiai neturi ko saugoti. ,,Įmonė nėra izoliuota nuo kitų įmonių ar organizacijų. Tiek verslo įmonės, tiek patys įrenginiai tampa vis labiau tarpusavyje susiję ir sujungti skaitmeniniu būdu, siekiant gerinti ar automatizuoti veiklos procesus. Išnaudodami tai, įsibrovėliai vis dažniau taikosi į mažesnių įmonių neapsaugotus tinklus ir įrenginius“ (Kibernetinio saugumo vadovas verslui, 2022).

Organizacijos verslo procesų valdymas yra nebeatsiejamas nuo IT. Naujosios IT palengvina, padeda efektyviau valdyti bei gerina verslo procesus. Šiuolaikinėje organizacijoje procesų taikymas, analizė, optimizavimas, matavimas ir valdymas, pagrįstas IT, tampa būtinomis sąlygomis norint užtikrinti organizacijos inovatyvumą bei konkurencingumą rinkoje (Ulbinaitė & Gribovskis, 2020). Verslo procesų efektyvumas veikia ir įmonės veiklos rezultatus. Įmonės veikloje vyksta daug vienas su kitu susijusių procesų. Remiantis Ulbinaite ir Gribovskiu (2020), ,,paprastai vieno proceso produkcija transformuojasi į kito proceso gavinius, taigi bet kurio proceso sutrikimas paveikia kitų procesų veiklą ir atitinkamai – rezultatus. Procesas į veiklų grandinę sujungia materialinius, finansinius ir žmogiškuosius išteklius, leidžiančius pasiekti, valdyti ir prognozuoti rezultatą.“ Dėl šios priežasties ne tik IT pagrindu valdomų verslo procesų kokybei, bet ir visos organizacijos pridėtinės veiklos kūrimui bei sėkmingam augimui - veiklos finansiniams ir ne finansiniams rezultatams, reikalingas kibernetinio saugumo užtikrinimas.

Verslo procesai yra įmonės veiklos pamatas. Dabartinės rinkos tendencijos skatina daugelį įmonių lanksčiau kurti savo verslo procesus, kad galima būtų greičiau reaguoti į besikeičiančius klientų poreikius. Verslo procesų lankstumas svarbus ir įmonėms užsitikrintini savo konkurencingumą rinkoje (Sackmann, 2008). Siekiant sukurti verslo procesų lankstumą stiprėja ir IT naudojimo vaidmuo. Didėjantis verslo procesų lankstumas, pagrįstas IT naudojimu, ne tik pagerina veiklos efektyvumą, bet ir padidina kibernetinių pavojų atsiradimą. Verslo procesai yra tiesiogiai susiję su įmonės ekonominės vertės augimu. Didėjanti verslo procesų priklausomybė nuo IT didina potencialius netiesioginius nuostolius, atsirandančius dėl IT

sistemų gedimo ar pažeidimo. Tačiau IT yra ne tik naujų rizikų šaltinis, bet ir daug žadanti pradinis taškas jų įvertinimui ir valdymui (Sackmann, 2008).

Didžioji dalis kiekvienos organizacijos funkcijų ir procesų įprastai priklauso nuo sistemų ir programinės įrangos. Bet koks šių sistemų ar programinės įrangos sutrikimas gali turėti rimtų padarinių įmonės veiklai: gali sutrikdyti verslo procesų tęstinumą; sukelti duomenų ir programinės įrangos praradimą; pabloginti produkto ar teikiamos paslaugos kokybę (klientai gali reikalauti, iškelti ieškinį dėl atsakomybės); sukelti fizinio turto (įrangos, programų sisteminės įrangos, mašinų) sugadinimą (OECD, 2017).

Remiantis Nacionalinio Kibernetinio saugumo informacija (2022) kibernetinių incidentų sukurti nuostoliai įmonėms apima:

- finansinius nuostolius dėl banko ar kitų finansinių duomenų praradimo arba pinigų vagysčių;
- finansinius nuostolius dėl vykdomos veiklos sutrikdymo;
- išlaidas, susijusias su paveiktų IT sistemų sutvarkymu, atkūrimu bei remontu;
- baudas dėl Bendrojo duomenų apsaugos reglamento nesilaikymo, kai yra asmens duomenų pažeidimų;
- teisininkų paslaugas;
- įmonės veiklai reikalingos informacijos praradimą ir jos atkūrimą;
- poveikį įmonės reputacijai ir klientų pasitikėjimo praradimą;
- žalą kitoms įmonėms ar kitiems verslo partneriams, kuriems teikiate savo prekes ar paslaugas.

Toliau lentelėje (žr. ***4* lentelė**) detaliau pateikiami galimi potencialūs nuostoliai įmonei paveiktai tam tikro tipo kibernetini incidento.

4 lentelė

Kibernetinių incidentų potencialūs nuostoliai

Kibernetinio incidento tipas	Potencialūs nuostoliai įmonei
Duomenų konfidencialumo pažeidimas	• Intelektinės nuosavybės vagystė; • Įmonės vadovų atsakomybė; • Trečiosios šalies duomenų konfidencialumo pažeidimas; • Reagavimo į incidentą išlaidos; • Kompensacijos už privatumą pažeidimą; • Žala reputacijai; • Teisinės išlaidos, baudos; • Įmonės vadovų atsakomybė.
Sistemos gedimas, problema	• Baudos; • Verslo procesų nutrūkimas; • Fizinio turto apgadinimas; • Įmonės vadovų atsakomybė; • Reagavimo į incidentą išlaidos; • Žala reputacijai; • Tinklo saugumo pažeidimo atsakomybė; • Teisinės išlaidos; • Nenumatytas verslo procesų nutrūkimas.
Duomenų prieinamumas	• Reagavimo į incidentą išlaidos; • Duomenų ir programinės įrangos praradimas; • Žala produkto/paslaugos kokybei; • Įmonės vadovų atsakomybė; • Kibernetinės išpirkos nuostoliai.
Kenkėjiška veikla	• Finansiniai nuostoliai; • Vagystė; • Įmonės vadovų atsakomybė.

Šaltinis: sudaryta autoriaus, remiantis OECD (2017).

Apžvelgus lentelę (žr. ***4* lentelė**), galima pastebėti, jog įvykęs bet kokio tipo kibernetinis incidentas užtikrina finansinius nuostolius, kuriuos sudaro ne tik tiesiogiai atakos metu prarasti pinigai, bet ir baudos, teisinės išlaidos. Taip pat, įmonės vadovų atsakomybė ir tiesiogiai susiję reputacinės žalos nuostoliai gali būti priskiriami prie vienų iš didžiausių galimų nuostolių įmonei paveiktai kibernetinio incidento.

Kiekvienos įmonės tikslas – kurti pridėtinę vertę ir sėkmingai vykdyti veiklą. Įmonės veiklos sėkmei ir efektyvumui pamatuoti reikalingas rezultatų vertinimas. Įmonės veiklos rezultatus galima įvertinti matuojant tiek finansinius, tiek ne finansinius įmonės veiklos aspektus. Finansiniai rezultatai siejami su tuo, kaip pelningai įmonė veikia. Finansiniai rezultatai išreiškiami įmonės pajamomis, pelnu, pardavimų, rinkos dalies tikslų įgyvendinimu. Ne finansiniai rezultatai susiję su kitų svarbių aspektų, tokių kaip, klientų pritraukimu ir išlaikymu, veiklos procesų efektyvumu, reputacija ir įvaizdžiu, konkurencingumu rinkoje (Tsou & Hsuan-Yu Hsu, 2015) (Blazevic & Lievens, 2004). Kibernetinio saugumo pasirengimas gali būti matuojamas remiantis NIST kibernetinio saugumo sistema, kurią sudaro pagrindiniai etapai (identifikuoti, apsaugoti, aptikti, atsakyti ir atsistatyti (Eilts, 2020).

Įvairiuose moksliniuose šaltiniuose aptariama organizacijos saugumo teigiama įtaka organizacijos rezultatams. Nustatyta, kad saugumo procesų užtikrinimas teigiamai veikia ilgalaikius įmonės finansinius ir nefinansinius rezultatus (Eccles, Ioannou, & Serafeim, 2014). Organizacijos užtikrindamos kibernetinį saugumą gali pasiekti geresnių finansinių rezultatų ir užsitikrinti geresnę reputaciją (Smith, Winchester, Bunker, & Jamieson, 2010) (Tsou & Hsuan-Yu Hsu, 2015). Kibernetinio saugumo taisyklės ir standartų laikymasis stiprina organizacijos saugumą, kuris taip pat prisideda prie geresnių įmonės veiklos rezultatų (Daud, Rasiah, George, Asirvatham, & Thangiah, 2018).

Taigi tam, kad būtų galima suvaldyti ar bent jau išvengti didelių nuostolių susijusių su kibernetiniais incidentais, kurie tiesiogiai gali paveikti verslo procesus bei pačios įmonės veiklos tęstinumą ir rezultatus, įmonės turėtų taikyti tinkamą kibernetinės rizikos valdymo sistemą ir priemones. Kibernetinis saugumas nėra baigtinis procesas ir jokia įmonė negali užtikrinti visiško atsparumo kibernetinėms grėsmėms (Nacionalinis kibernetinio saugumo centras, 2022), tačiau taikant atitinkamas priemones ir procedūras galima sumažinti jų poveikį ir vystyti savo organizacijos saugumo reputaciją bei pasiekti geresnių finansinių ir nefinansinių veiklos rezultatų.

1.6 Labiausiai kibernetinių atakų paveikti sektoriai

Įvairaus dydžio ir verslo sektorių įmonės tampa kibernetinių atakų aukomis. Remiantis Bendovschi (2015) tyrimu, nepriklausomai nuo subjekto dydžio, dažniausiai nuo kibernetiniu atakų nukenčia viešojo sektoriaus sritys (vyriausybė, teisė, švietimas, sveikatos apsauga) ir privataus sektoriaus įmonės veikiančios finansų, žiniasklaidos, internetinių paslaugos, turizmo, telekomunikacijų, mažmeninės prekybos, švietimo srityse. Nacionalinio kibernetinio saugumo centro pranešimo duomenimis (LR rašto apsaugos Ministerija, 2022), kibernetinių incidentų

rizika yra didelė, ypač, prieš Lietuvos ypatingos svarbos informacines infrastruktūras ir valstybės informacinius išteklius.

Apibendrinus Benson (2017) ataskaitos rezultatus, daroma išvada, jog viešasis sektorius ir toliau dominuoja kaip pagrindinis kibernetinių atakų taikinys, po kurio eina finansinės paslaugos. Finansų ir banko bei draudimo sektoriaus įmonės apibūdinamas kaip labiausiai nukenčiančios nuo kibernetinių atakų ir Bouveret Tarptautinio Valiutos Fondo (2018) knygoje. Taip pat, pagal dažnumą, finansinė ir draudimo veikla yra labiausiai paveiktas sektorius, tačiau vidutiniškai patiria mažesnes išlaidas. (Aldasoro, Gambacorta, Giudici, & Leach., The drivers of cyber risk, 2022).

Finansines technologijos (Fintech) nulėmė spartų inovacijų augimą ir pakeitė visą finansų sektoriaus ekosistemą. Fintech paskatino finansų sektoriaus transformaciją, bet kartu su didėjančia priklausomybe nuo skaitmeninių finansų produktų ir inovacijų padidėjo finansų sektoriaus kibernetinė rizika - pažeidžiamumas kibernetinėms atakoms. Augant Fintech pažangai didėja ir kibernetinio saugumo poreikis (Callen-Naviglia & James, 2018). Finansinės institucijos (tokios kaip bankai) vis daugiau investuoja į finansines technologijas su tikslu pagerinti finansines paslaugas ir veiklos procesus, todėl tampa Fintech ekosistemos dalimi (Adeyoju, 2019). Fintech startuoliai, bankai ir kitos finansų institucijos, kurios naudoja finansines technologijas, taip pat susiduria su didėjančia kibernetine rizika. Didėjant ir augant Fintech įmonėms didėja ir jų įtaka visai finansų sistemai, tai reiškia, jog pažeidžiamumai susiję su Fintech gali turėti padarinių visai finansų sistemai. Fintech susiduria su išaugusia kibernetine rizika, nes yra labai priklausomos nuo technologijų ir duomenų – šie faktoriai sukuria palankias sąlygas kibernetinėms atakoms. To priežastis yra Fintech tendencijos atsisakyti įprasto autentifikavimo (tokias priemones kaip slaptažodžiai ir asmeniniai identifikavimo numeriai) ir pasikliauti daugiau biometriniais jutikliais, vienkartiniais slaptažodžiais, kodais ir. kt (Adeyoju, 2019). Taip didėja duomenų vientisumo, atskleidimo ir kenkėjiškų programų atakų rizika. „Fintech“ šūkis „duomenys yra naujoji valiuta“ iškart asocijuojasi su išaugusia kibernetine rizika (Allen, Gu, & Jagtiani, 2020). Dėl šių priežasčių kibernetinis saugumas turėtų būti prioritetas Fintech sektoriaus įmonėse. Kibernetinės atakos gali atgrasyti nuo Fintech diegimo ir naudojimo, todėl būtina imtis proaktyvių kibernetinių saugumo priemonių – kurios gyvuotų per visą produktų/paslaugų gyvavimo ciklą (Faya & Ogbuefi, 2019). Užtikrintas kibernetinis saugumas Fintech sektoriuje ne tik paskatintų didesnį pasitikėjimą finansinėmis technologijomis, bet ir prisidėtų prie finansų sektoriaus tolimesnio vystymosi.

1.7 Finansinių technologijų sektorius Lietuvoje

Finansinės technologijos (Fintech) – tai technologijomis pagrįstos finansinės inovacijos, padedančios kurti naujus verslo modelius, veiklos programas, procesus ir produktus (Lietuvos Bankas, 2022). Paprasčiau įvardijant, Fintech apibūdinama įmonė, kurios tikslas teikti finansines paslaugas, naudojant programinę įrangą ir šiuolaikines technologijas (Malčiauskaitė & Kvietkauskienė, 2019). Šios inovacijos turi reikšmingą poveikį finansų rinkoms, institucijoms ir finansinėms paslaugoms.

Finansų technologijų (FinTech) sektoriaus dalyviai teikia inovatyvias paslaugas verslui ir vartotojams ir didina konkurencinį spaudimą. Šiame sektoriuje kuriamos aukštos pridėtinės vertės darbo vietos, mokami mokesčiai į valstybės biudžetą, prisidedama prie platesnės startuolių ekosistemos vystymo šalyje (Lietuvos Bankas, 2021).

Pagal Investuok Lietuvoje ataskaitą (2022), per pastaruosius metus Lietuvos Fintech sektorius pasiekė didžiausias aukštumas. Šiuo metu Lietuvoje veikia 256 finansinių technologijų įmonės, kuriose dirba apie 6000 žmonių.

Fintech įmonių skaičius Lietuvoje kasmet toliau auga, nes metams bėgant yra išlaikoma stipri Fintech ekosistema dėl:

- Fintech draugiško reguliavimo ir gerai išvystytos infrastruktūros;
- Patogumo kurti verslą;
- Taip viena iš Fintech augimo priežasčių Lietuvoje yra šios industrijos darbuotojų, talentų pasiekiamumas.

Lietuvos finansinių technologijų sektoriaus augimas nebuvo atsitiktinis. 2016 metais Lietuvos Bankas ir kitos valstybinės institucijos pristatė šalies Fintech strategiją, kurios tikslas skatinti finansinių technologijų ekosistemos augimą. Šis strateginis požiūris padėjo sukurti atitinkamą reglamentavimą ir infrastruktūra Fintech įmonėms Lietuvoje (Invest Lithuania, 2022). Fintech reguliavimo ir priežiūros ekosistemos plėtra bei inovacijų finansų sistemoje skatinimas yra viena iš Lietuvos banko strateginių krypčių (Lietuvos Bankas, 2022).

Daugiau nei trečdalis Fintech įmonių įvardiją politiką, mokesčių lengvatas ir bandomąją finansinių inovacijų aplinką kaip finansinių technologijų ekosistemos Lietuvoje pranašumus.

Lentelėje (žr. **5 lentelė**) pateikiamos Lietuvos Banko priemonės, kuriomis siekiama pritraukti naujas Fintech įmones ir skatinti jas kurti naujus finansinių technologijų produktus Lietuvoje.

5 lentelė

Lietuvos Banko priemonės Fintech įmonių skatinimui

Priemonės pavadinimas	**Paaiškinimas**
Rinkos naujokams	Vieno langelio principu pagrįsta programa, skirta: • susitikimams ir konsultacijoms su potencialiais finansų rinkos dalyviais organizuoti; • pagrindinei informacijai apie licencijavimo ir finansinių paslaugų galimybes Lietuvoje teikti; • užklausoms dėl susitikimų ir konsultacijų el. paštu ar telefonu, norint pradėti verslą ar kurti naują produktą, teikti; • galimybei pasitikrinti, ar ateities planai atitinka teisinius ir licencijavimo reikalavimus, sudaryti.
Bandomoji finansinių inovacijų aplinka	Suteikia galimybę inovatyvių finansinių produktų ir verslo sprendimų kūrėjams išbandyti juos realioje aplinkoje, Lietuvos bankui prižiūrint ir teikiant konsultacinę pagalbą.
Reguliavimo technologijos	Pagrindines kryptis, kuriose Lietuvos bankas galėtų įdiegti RegTech sprendimus, išgrynintos diskusijose su finansų rinka, informacinių technologijų, akademine bendruomene, viešojo sektoriaus atstovais.
Atviroji bankininkystė	Atviroji bankininkystė yra pagrįsta skirtingų finansų įstaigų technologiniu tinklu, leidžiančiu joms efektyviau keistis informacija. 2018 m. lapkritį Lietuvos bankas paskelbė viešą konsultaciją dėl atvirosios bankininkystės.

Šaltinis: sudaryta autoriaus, remiantis Lietuvos Banku (2022).

Nuolat skiriamas dėmesys verslo gerinimui ir reguliavimo aplinka, padeda Lietuvai tapti vienai iš geriausių besivystančių finansinių technologijų ekosistemų. Taip pat siekiant gerinti Fintech sektoriaus įmonių integraciją yra sukurtos tokios organizacijos kaip „Fintech Lietuvoje“ ir „ROCKIT Lietuva“, kurios vienija finansinių technologijų įmonės ir skatina jų bendradarbiavimą.

Nors ir Lietuva pasižymi dideliu finansiniu technologijų įmonių skaičiumi, jų siūlomi produktai ir paslaugos gerina finansinių paslaugų teikimą, šios įmonės vis dar turi nevisišką visuomenės pasitikėjimą. Kibernetiniai incidentai, kurių metu nukenčia konfidencialūs ir jautrūs klientų duomenis, verčia žmones atsakingiau pagalvoti prieš naudojantis tam tikra paslauga.

Apibendrinant pirmąją darbo dalį, galima teigti, kad kibernetinės rizika tai yra rizika, atsiradusi dėl informacijos ir ryšių technologijų sukeltų pavojų duomenų ir paslaugų konfidencialumui, prieinamumui ir vientisumui. Kibernetiniai incidentai gali įvykti dėl žmogaus klaidos, stichinių nelaimių ar programų gedimo. Pagrindiniai kibernetinių incidentų tipai yra: duomenų konfidencialumo pažeidimas; sistemos gedimas, problema; duomenų prieinamumas; kenkėjiška veikla. Kibernetiniai incidentai gali turėti didelių neigiamų padarinių įmonei, klientams bei su ja susijusiems subjektams, nes įmonė gali ne tik prarasti sistemas, duomenis, įrangą, bet ir patirti didelių finansinių nuostolių, susigadinti reputaciją bei susidurti su teisine atsakomybe. Šiuolaikinės organizacijos tampa priklausomos nuo skaitmeninės informacijos, todėl tai ne tik gerina verslo procesų efektyvumą, bet ir didina kibernetinę riziką. Finansų sektoriaus, ypač finansinių technologijų įmonės išskiriamos kaip labiausiai nukenčiančios nuo kibernetinių atakų dėl technologiniu pagrindu grįstų finansinių sprendimų ir duomenų svarbumo. Įmonės, norėdamos užtikrinti savo veiklos tęstinumą bei užkirsti kelią ar bent sumažinti potencialus nuostolius, turi užtikrinti kibernetinio saugumo priemones ir gerinti kibernetinio saugumo pasirengimą stiprinančius veiksnius. Pagrindiniai kibernetinio saugumo veiksniai apima technologinius, organizacinius ir aplinkos veiksnius. Šie veiksniai gerina įmonių pasirengimą atremti kibernetines atakas. Organizacijos finansinių ir ne finansinių rezultatų sėkmė priklauso ne tik nuo įmonės procesų kokybės ir efektyvumo bei kitų aspektų, bet ir nuo jos pasirengimo valdyti kibernetinę riziką.

2. KIBERNETINIO SAUGUMO ĮTAKOS FINTECH ĮMONIŲ VEIKLOS REZULTATAMS TYRIMO METODIKA

Šis skyrius skirtas tyrimo metodologijos aprašymui. Šiame skyriuje atliktos mokslinės analizės pagrindu apibrėžiama tyrimo sritis, tikslas ir uždaviniai. Aprašomi naudojami metodai ir jų pagrindimas, tyrimo planas ir apribojimai bei įvardijami tyrime dalyvaujantys respondentai.

Atlikta mokslinių šaltinių analizė parodė, jog daugiausia tyrimų susijusių su kibernetiniais incidentais ir kibernetinio saugumo tema yra nukreipti į kibernetinių incidentų klasifikaciją, jų dažnumą, kibernetinių incidentų nuostolius. Taip pat nemažai tyrimų nagrinėja kibernetinių incidentų priežastis ir faktorius. Kelių tyrimų pagrindiniai aspektai pateikti lentelėje (žr. ***6*** **lentelė**).

6 lentelė

Mokslinių tyrimų, kibernetinio saugumo tema, analizė

Autorius, metai	**Pavadinimas**	**Metodas**	**Tyrimo sritis**	**Respondentai**
(Maharjan & Chatterjee, 2019)	,,Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal“	Mišrus – kokybinis ir kokybinis metodas	Kibernetinio saugumo grėsmės	Finansinės ir valdžios institucijos
(Shaikha, Ali, Kurnia, & Thurasamy, 2021)	,,Evaluating the cyber security readiness of organizations and its influence on performance“	Kiekybinis metodas (apklausa) modelio hipotezėms patikrinti	Faktoriai lemiantys pasirengimą kibernetiniam saugumui	IT srities darbuotojai (900)
(Lallie, et al., 2021)	,,Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic.“	Kokybinis metodas. Pranešimų ir kitų šaltinių peržiūra, analizė.	Kibernetinių atakų diapazonas	Paieškos sistemos, naudojami raktažodžiai
(Ali, 2019)	,,Cyber crimes-A constant threat for the business sectors and its growth (A study of the online banking sectors in GCC).“	Kiekybinis metodas – apklausa.	Kibernetinių nusikaltimų veiksniai, darantys įtaką banko sektoriaus augimui	Bankininkų ir finansų sektoriaus darbuotojai GCC šalyse

(Héroux & Fortin, 2020)	,,Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index.“	Kokybinis metodas. Įmonių pranešimų ir kitų šaltinių naujienų analizė.	Kibernetinio saugumo incidentų atskleidimo apimties vertinimas	Bendrovės įtrauktos į S & P / TSX 60 indeksą Toronto vertybinių popierių biržoje (TSX)
(Jevsejev, 2020)	,,Informacinių technologijų rizikos vertinimo metodai ir tobulinimo sprendimai“	Kiekybinė apklausa ir kokybinis interviu, dokumentų analizė	IT rizikos vertinimo metodai	IT specialistai
(Eling & Wirfs, 2019)	,,What are the actual costs of cyber risk events?“	Kiekybinė duomenų analizė	Kibernetinių incidentų mastas ir nuostoliai	Vieši (SAS OpRisk Global)duomenys
(Aldasoro, Gambacorta, Giudici, & Leach, 2022)	,,The drivers of cyber risk“	Kiekybinė duomenų analizė	Kibernetinių incidentų ypatybės ir veiksniai	3705 kibernetiniai incidentai (JAV visuose ekonomikos sektoriuose)
(Elnagdy, Qiu, & Gai, 2016)	,,Cyber Incident Classifications Using Ontology-Based Knowledge Representation for Cybersecurity Insurance in Financial Industry“	Semantinės kibernetinių incidentų klasifikacijos (SCIC) modelis	Kibernetinių incidentų klasifikacija	Atvejo analizė
(Kuklytė & Ūsas, 2017)	,,Informacinės visuomenės iššūkiai: kokios yra kibernetinių nusikaltimų formos?“	Literatūros analizė ir sintezė, chronologija, analogija	Kibernetinių nusikaltimų formos	Literatūros šaltiniai

Šaltinis: sudaryta autoriaus.

Moksliniuose šaltiniuose nemažai dėmesio skiriama viešojo bei finansų ir banko sektoriams, kurie įvardijami kaip vieni iš labiausiai paveiktų kibernetinių atakų. Užsienio moksliniuose tyrimuose yra atlikta tyrimų nagrinėjančių finansų ir bankų sektorių kibernetinius incidentus ir saugumą, tačiau Lietuvos mastu tokių tyrimų – mažai.

Moksliniuose straipsniuose įvardijama, jog finansinių technologijų (Fintech) įmonių sukurtos naujovės patobulino ir pakeitė tradicines finansines paslaugas, tačiau kibernetinė rizika yra viena didžiausių tokias įmones veikiančių rizikų. Finansinių inovacijų tempas yra spartus, bet kartu su jomis auga ir kibernetinių incidentų rizika (Milena & Radoica, 2022). Taip pat

įvardijama, jog Fintech sektorius yra labai jautrus kibernetinėms atakoms susijusiomis su duomenų pažeidžiamumu, o laiku nustatyti duomenų pažeidimai ir tinkamas kibernetinio saugumo elementų taikymas gali paskatinti tolimesnį finansinių technologijų vystymąsi (Umara, Anwar, Amjad, & Raymond, 2019). Finansinių technologijų įmonės įvardijamos ir kaip finansų sektoriaus variklis, kuris skatina ne tik didina konkurencingumą rinkoje, tačiau ir skatina tokias institucijas kaip bankus diegti naujoves (Panetta, 2018).

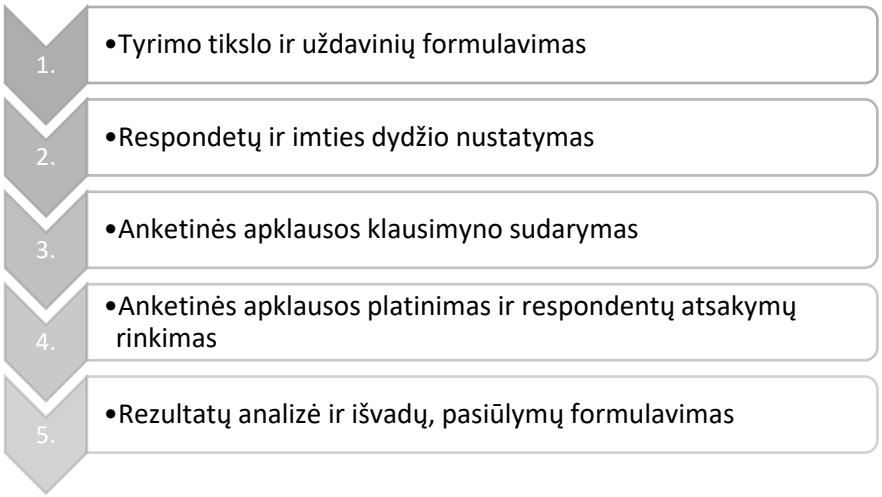
Apibendrinus, kokybiškų tyrimų kibernetinės rizikos ir saugumo temą finansinių technologijų įmonėse nagrinėjančių yra gana mažai, Lietuvos mastu tai išvis mažai išnagrinėta sritis ir daugiau išanalizuota tik iš teorinės pusės.

Vis didėjantis IT naudojimas įmonių verslo procesuose neabejotinai didina ir kibernetinės rizikos reikšmę organizacijose. Dabartinėje įmones veikiančioje aplinkoje ne tik didėja kibernetinių atakų skaičius, bet auga ir jų sudėtingumas. Fintech įmonės yra finansinio sektoriaus inovacijų variklis ir yra pagrįstos IT, todėl yra labai veikiamos kibernetinės rizikos. Šiuo empiriniu tyrimu siekiama išsiaiškinti finansinių technologijų sektoriaus įmonių kibernetinio saugumo veiksnius ir kibernetinės rizikos valdymo įtaką veiklos rezultatams.

Atlikto tyrimo eiga pavaizduota paveiksle (žr. **4 paveikslas**).

4 paveikslas

Tyrimo eiga



Šaltinis: sudaryta autoriaus.

Tyrimo eiga sudaryta iš penkių pagrindinių etapų. Pirmiausia suformuluojami tyrimo tikslai ir uždaviniai tikslui pasiekti. Toliau aprašomi respondentai ir nustatoma imtis. Atsižvelgiant į ankstesnius tyrimus ir tyrimo uždavinius sudaroma anketinė apklausa. Ši

apklausa platinama elektroniniu būdu iki kol pasiekiamas reikiamas respondentų atsakymų skaičius. Gauti rezultatai apdorojami, analizuojami ir pateikiamos išvados ir pasiūlymai.

Tyrimo objektas – kibernetinio saugumo veiksniai, įmonių veiklos rezultatai.

Tyrimo vienetai – Fintech sektoriaus įmonės Lietuvoje.

Tyrimo tikslas – išsiaiškinti kibernetinio saugumo įtaką veiklos rezultatams Fintech sektoriaus įmonėse Lietuvoje.

Tikslui pasiekti suformuoti **tyrimo uždaviniai**:

1. Išsiaiškinti, kokie pagrindiniai veiksniai turi įtakos kibernetinio saugumo pasirengimui Fintech sektoriaus įmonėse.
2. Išskirti aktualiausius kibernetinio saugumo veiksnius Fintech sektoriaus įmonėse.
3. Išsiaiškinti, kaip Fintech sektoriaus įmonių pasirengimas kibernetiniam saugumui daro įtaką finansiniams bei ne finansiniams veiklos rezultatams.
4. Atlikus tyrimą, pateikti rekomendacijų Fintech įmonių Lietuvoje kibernetinio saugumo veiksnių gerinimui, kad būtų sumažintas kibernetinių atakų pasireiškimas ir poveikis.

2.1 Tyrimo imtis ir respondentai

Remiantis moksliniu šaltinių analize, jog finansinis sektorius, o ypač finansinių technologijų įmonės apibūdinamos kaip labiausiai veikiamos kibernetinių atakų, tyrimui atlikti buvo nuspręsta pasirinkti Lietuvos Fintech sektorių.

Tyrimo respondentai – Lietuvoje veikiančių Fintech bendrovių generaliniai direktoriai, direktoriai, IT skyrių vadovai, saugumo vadovai ir specialistai bei kiti aukšto lygio vadovai.

Remiantis „Investuok Lietuvoje“ kasmetinės Fintech sektoriaus apžvalgos duomenimis (Invest Lithuania, 2022), 2021 metų pabaigoje Lietuvoje buvo 256 Fintech bendrovės. Lietuvoje veikiančias Fintech bendroves galima suskirstyti į kategorijas pagal veiklos sritį:

- Skaitmeninė bankininkystė
- Mokėjimai
- Skolinimas
- Taupymas ir investavimas
- „Insurtech“
- Didieji duomenys ir analitika

- Finansinė programinė įranga
- Atitikties valdymas ir kibernetinis saugumas
- „Blokchain“ ir kripto valiutos
- Kitos

Imties dydžio nustatymui naudojama V.I. Pannioti imties dydžio formulė (Valackienė, 2007):

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

čia: n – imties dydis;
Δ – imties paklaidos dydis arba ribinė atrankos paklaida;
N – tyrinėjamos populiacijos dydis.

Atsižvelgiant į tai, jog socialinių mokslų tyrimuose priimtina 10 % paklaida (Δ = 0,1), tyrimo metu siekiama surinkti 72 respondentų iš skirtingų Fintech įmonių Lietuvoje atsakymų, tam kad imtis užtikrintų bent 90% patikimumo tikimybę.

2.2 Tyrimo metodas

Išanalizavus atliktus tyrimus IT saugos rizikos tema, pastebėta tendencija, jog dažniausiai autorių buvo pasirinktas kiekybinis tyrimas apklausos forma arba kokybinis tyrimas interviu metodu. Atsižvelgiant į šio darbo tyrimo tikslą buvo nuspręsta, kad siekiama išnagrinėti grupės (Fintech įmonių Lietuvoje) rezultatus, kurie galėtų apibendrinti ir atspindėti populiacijos nuomonę, tendencijas. Tyrimu norima pagrįsti objekto požymius, reiškinių priežastinius ryšius, todėl darbo tikslo pasiekimui tinkamesnis kiekybinis tyrimas.

Atlikta mokslinių tyrimų ir literatūros analizė išryškino svarbiausius kibernetinio saugumo veiksnius - organizacijos pasirengimas kibernetiniam saugumui priklauso nuo: IT infrastruktūros, aukščiausios vadovybės palaikymo, organizacijos įgūdžių ir kultūros, bendradarbiavimo su konkurentais, santykių su partneriais, valstybės reguliavimo ir paramos, pramonės šakos standartų laikymosi. Visi šie veiksniai tyrime naudojami kaip konstruktai. Siekiant išsiaiškinti jų įtaką kibernetinio saugumo pasirengimui ir įmonės veiklos rezultatams, papildomai tyrimui naudojami šie konstruktai: kibernetinio saugumo pasirengimas, organizacijos saugumas, finansiniai rezultatai ir ne finansiniai rezultatai. Tyrimui atlikti visi naudojami konstruktai ir jų paaiškinimai, pateikti lentelėje (žr. ***7* lentelė**).

7 lentelė

Tyrimo konstruktų paaiškinimas

Konstruktas	Paaiškinimas
IT Infrastruktūra (IT)	IT resursų prieinamumas ir naudojimas organizacijoje kibernetiniam saugumui užtikrinti.
Organizacijos kultūra (OK)	Aukščiausiųjų organizacijos vadovų įsipareigojimas ir parama kibernetinio saugumo palaikymui ir stiprinimui; Organizacijos vertybės ir įsitikinimai, susiję su kibernetiniu saugumu.
Darbuotojų įgūdžiai (DI)	Darbuotojų įgūdžiai kibernetinės saugos tema organizacijos viduje.
Bendradarbiavimas su konkurentais ir partneriais (BKP)	Organizacijos bendradarbiavimas su rinkos konkurentus, kibernetinio saugumo gerinimui. Organizacijos bendradarbiavimas su partneriais, kibernetinio saugumo gerinimui.
Valstybės reguliavimas ir pramonės šakos standartai (VRPS)	Valstybės lygiu nustatytos taisyklės, kuriais reikalaujama stiprinti organizacijų kibernetinį saugumą. Tarptautinių institucijų nustatyti standartai organizacijų kibernetiniam saugumui.
Kibernetinio saugumo pasirengimas (KS)	Organizacijos pasirengimas kibernetinių atakų prevencijai ir atsakui.
Organizacijos saugumo efektyvumas (OS)	Kibernetinio saugumo efektyvumas numatomas dėl organizacijos kibernetinio saugumo pasirengimo.
Finansiniai rezultatai (FR)	Finansinė nauda numatoma dėl organizacijos saugumo efektyvumo.
Ne finansiniai rezultatai (NFR)	Ne finansinė nauda numatoma dėl organizacijos saugumo efektyvumo.

Šaltinis: sudaryta autoriaus remiantis (Hasan, Ali, & Kurnia, 2021).

Suformuluotos tyrimo hipotezės:

H1 (IT→ KS): Kuo brandesnė organizacijos IT infrastruktūra, tuo geresnis organizacijos pasirengimas kovoti su kibernetinėmis atakomis.

H2 (OK→ KS): Kuo stipresnė aukščiausios vadovybės parama kibernetiniam saugumui ir stipresnis kultūrinis kibernetinio saugumo palaikymas organizacijoje, tuo geresnis organizacijos pasirengimas kovoti su kibernetinėmis atakomis.

H3 (DI→ KS): Kuo stipresni organizacijos darbuotojų kibernetinio saugumo valdymo įgūdžiai, tuo geresnis organizacijos pasirengimas kovoti su kibernetinėmis atakomis.

H4 (BKP→ KS): Kuo aktyvesnis organizacijos bendradarbiavimas su konkurentais ir partneriais, tuo geresnis jos pasirengimas kovoti su kibernetinėmis atakomis.

H5 (VRPS → KS): Vyriausybės parama ir reglamentai, susiję su kibernetiniu saugumu, ir kibernetinio saugumo standartų laikymasis gerina organizacijų pasirengimą kovoti su kibernetinėmis atakomis.

H6 (KS→ S): Kuo didesnis organizacijos pasirengimas kovoti su kibernetinėmis atakomis, tuo didesnis organizacijos kibernetinio saugumo efektyvumas.

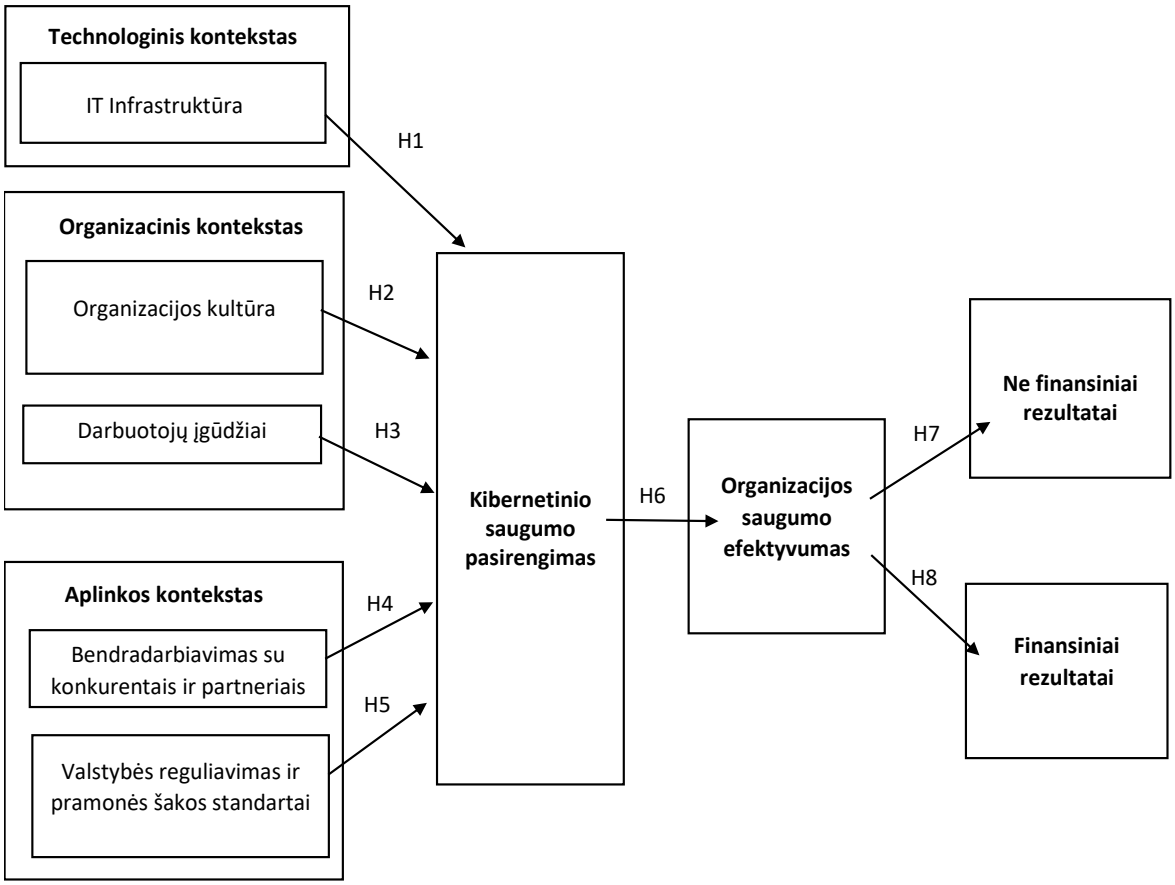
H7(S→ FR): Didesnis organizacijos kibernetinio saugumo efektyvumas yra susijęs su aukštesniais finansiniais rezultatais.

H8 (S → NFR): Didesnis organizacijos saugumo efektyvumas yra susijęs su aukštesniais nefinansiniais rezultatais.

Tyrimo modelis, kuriame pavaizduotas ryšis tarp konstruktų, pateiktas paveiksle (žr. **5 paveikslas**).

5 paveikslas

Tyrimo modelis



Šaltinis: sudaryta autoriaus, remiantis (Hasan, Ali, & Kurnia, 2021).

Empirinio tyrimo atlikimui pasirinktas kiekybinio tyrimo metodas - struktūruota anketinė apklausa. Struktūruota anketa respondentams pateikiama elektronine forma, todėl yra respondento administruojama. Pagal pasirinktą tyrimo modelį iš konstruktų teiginių buvo atrinkta tik dalis, tam, kad galima būtų sumažinti apklausos apimtį. Pradiniai konstruktai ir teiginiai pateikti prieduose (žr. **1 priedas**).

Anketinės apklausos klausimai/teiginiai buvo atrinkti, suformuoti ir pritaikyti, kad padėtų įvykdyti užsibrėžtus tyrimo uždavinius. Pradinė anketa buvo sudaryta iš 72 teiginių. Iš pradžių jų skaičius buvo sumažintas iki 39, tačiau galutinė apklausos anketa buvo suformuota iš 26 tyrimo klausimų/teiginių, kurie buvo pateikiami tyrimo respondentams.

Respondentų buvo prašoma įvertinti konstruktų teiginius naudojant penkiabalę Likerto skalę (1 = "visiškai nesutinku", 2 = "nesutinku", 3 = "neutralus", 4= „sutinku“, 5 = „visiškai sutinku“). Tyrimo anketos pateikta prieduose (žr. **2 priedas**).

2.3 Tyrimo apribojimai

Respondentų atsakymai į anketų klausimus renkami 2022 spalio – lapkričio mėn. laikotarpiu. Tyrime respondentai dalyvauja savanorišku principu. Prieš dalyvavimą respondentai informuojami apie surinktų duomenų panaudojimą tyrimo tikslams ir supažindinami su tyrimo uždaviniais. Sukurta internetinė apklausa naudojant „Google forms“ platinama respondentams elektroniniu būdu, daugiausia naudojant socialinį tinklą „Linkedin“, taip pat anketinės apklausos buvo siunčiamos respondentams el. paštu. Respondentai buvo kontaktuojami remiantis Fintech įmonių Lietuvoje duomenų baze (ROCKIT VILNIUS, 2022). Buvo sukurtos dvi anketos - lietuvių ir anglų kalbomis.

2.4 Analizės metodai

Analizuojant metodologinius temos aspektus naudojama mokslinės literatūros ir tyrimų analizė. Iškeltiems tyrimo uždaviniams įgyvendinti naudojama aprašomoji statistika, koreliacinė ir regresinė analizė. Duomenų apdorojimo procedūroms naudojami SPSS ir MS Excel įrankiai.

Gautų tyrimo rezultatų sisteminimui ir grafiniam atvaizdavimui naudojama aprašomoji statistika. Prieš atliekant surinktų duomenų koreliacinę ir regresinę analizę, pirmiausia apžvelgiami gauti rezultatai, kiekvienas anketos teiginio rezultatas nagrinėjamas atskirai (Bilevičienė & Jonušauskas, 2011). Naudojamos dažnių lentelės ir diagramos, kurios parodo gautų tyrimo rezultatų pasiskirstymą. Tokiu pagrindu aprašomos pirmosios tyrimo rezultatų

įžvalgos. Taip pat skaičiuojami kintamųjų statistiniai įverčiai – vidurkis, standartinis nuokrypis, moda, mediana.

Tyrimui naudojami teiginiai sudaryti remiantis Likerto skale, todėl analizės metu sudedami vieno respondento atsakymai į visus teiginius ir skaičiuojamas vidurkis. Toks metodas leidžia įvertinti bendrą respondento nuomonę apie tyrimo objektus (konstruktus) ir nustatyti, kurie iš jų yra vertinami pozityviau. Taip transformuoti Likerto skalės ranginiai duomenys tampa intervaliniais ir yra naudojami koreliacinei bei regresinei analizei.

Ryšiui tarp tyrime iškeltų konstruktų nustatyti naudojama koreliacinė analizė. Koreliacinė analizė (koeficientas) – yra kintamųjų tiesinės priklausomybės matas (Čekanavičius & Murauskas, 2014). Atliekant koreliacinę analizę darbe skaičiuojami kintamųjų Spearmano ir Pearsono koreliacijos koeficientai.

Koreliacijos koeficiento reikšmės gali įgyti reikšmes intervale [-1;1]. Jei koreliacijos koeficientas 0 – ryšio taro kintamųjų nėra. Koreliacijos koeficiento reikšmių interpretacija įvardinta lentelėje žemiau (žr. ***8 lentelė***).

8 lentelė

Koreliacijos koeficiento reikšmės

Koreliacijos koeficiento reikšmė	**Interpretacija**
$\|r\| < 0,3$	labai silpna koreliacija
$0,3 \leq \|r\| < 0,5$	silpna koreliacija
$0,5 \leq \|r\| < 0,7$	vidutinė koreliacija
$0,7 \leq \|r\| < 0,9$	stipri koreliacija
$0,9 \leq \|r\| < 1$	labai stipri koreliacija

Sudaryta autoriaus, remiantis (Čekanavičius & Murauskas, 2014).

Koreliacijos koeficiento ženklas parodo kintamųjų priklausomybę:

- jei koeficiento reikšmės neigiamos, tai taro kintamųjų yra netiesioginė priklausomybė – vienam didėjant, kitas mažėja;
- jei koeficiento reikšmės teigiamos, tai tarp kintamųjų yra tiesioginė priklausomybė – vienam didėjant, didėja ir kitas.

Kintamųjų koreliacija dar nerodo priežastingumo, todėl iškeltų tyrimo hipotezių tikrinimui naudojama tiesinė regresinė analizė. Tiesinė regresinė analizė skirta nustatyti, ar nepriklausomi kintamieji turi įtakos priklausomam kintamajam – ieškomi priklausomo kintamojo regresoriai.

Atliekant regresinę analizę skaičiuojami modelio beta (b) koeficientai, kurių ženklai parodo ar didėjant regresoriam, didės ar mažės priklausomo kintamojo reikšmės (Čekanavičius & Murauskas, 2014):

- jei $b > 0$, tai nepriklausomam kintamajam didėjant, didėja ir priklausomas kintamasis;
- jei $b < 0$ nepriklausomam kintamajam didėjant, priklausomas kintamasis mažėja.

Atliekant analizę yra skaičiuojamas ir standartizuotas beta koeficientas. Kuo šis koeficientas didesnis, tuo atitinkamo nepriklausomo kintamojo įtaka priklausomam kintamajam modelyje didesnė. Šis koeficientas neinterpretuojamas jei modelyje yra tik vienas regresorius.

Modelio tinkamumui įvertinti naudojami šie rodikliai (Čekanavičius & Murauskas, 2014):

- Determinacijos koeficientas (R^2) – modelio tinkamumo duomenims charakteristika, kuri parodo kiek procentų priklausomo kintamojo elgesio paaiškina nepriklausomų kintamųjų elgesys. Koeficientas įgyją reikšmes iš intervalo [0;1], didesnės reikšmės rodo geresnį modelio tinkamumą duomenims.
- ANOVA p reikšmė - parodo ar modelyje yra regresorių priklausomam kintamajam. Jei $p < 0,05$, galima sakyti, jog modelyje yra su priklausomu kintamuoju susijusių regresorių.
- T (Stjudento) kriterijai – labai svarbus rodiklis, kuris rodo ar regresorius yra statistiškai reikšmingas modelyje. Jei T reikšmė $< 0,05$, tai regresorius statistiskai reikšmingas ir yra paliekamas modelyje.

3. TYRIMO REZULTATŲ ANALIZĖ

Šiame skyriuje pateikiama atlikto tyrimo rezultatų analizė - pateikiamas rezultatų aprašymas, atliekama koreliacinė ir regresinė analizė siekiant įgyvendinti tyrimo tikslą ir iškeltus uždavinius, kurių pagrindu formuojamos darbo išvados ir rekomendacijos.

3.1 Aprašomoji tyrimo rezultatų statistika

Tyrimo metu surinkti apklausos atsakymai iš 72 skirtingų Fintech įmonių Lietuvoje atstovų – užsibrėžta tyrimo imtis įgyvendinta. Tyrime dalyvavę įmonių atstovai užpildė apklausą el. formatu. Dauguma anketų (67) buvo užpildytos lietuvių kalba, likusi dalis (5) – anglų kalba. Tyrimo dalyviai įvertino 26 teiginius, apibūdinančius tyrimo modelyje apibrėžtus konstruktus. Priede pateikti visi atsakymų rezultatai bei pagrindiniai jų statistiniai rodikliai (žr. **3 priedas**).

Geriausiai Fintech įmonių atstovai dalyvavę tyrime, įvertino teiginį „Mūsų organizacija žino ir yra įsipareigojusi naudoti duomenų šifravimą, apsaugos nuo virusų programinę įrangą ir laikytis griežtos slaptažodžių politikos“. Su šiuo teiginiu visiškai sutiko/sutiko net 66 įmonės iš 72. Tai rodo, kad beveik visos įmonės įgyvendina pagrindines apsaugos nuo kibernetinių atakų priemones.

Taip pat stipriai įvertinti teiginiai, susiję su Fintech įmonių pasirengimu reaguoti į kibernetines atakas bei ir atsistatyti po jų. Net 64 įmonės nuolat stebėti saugos įspėjimus, ir yra pasirengusios reaguoti į kibernetines atakas, o 62 – turi atkūrimo plano procedūras. Šiek tiek prasčiau Fintech įmonės įvertino kibernetinių atakų identifikavimo priemonę – pažeidžiamumo vertinimą. Tik 59 įmonės įvardino, jog naudoja pažangius pažeidžiamumo vertinimo metodus.

Prasčiausiai įvertintas teiginys „Mūsų organizacija bendradarbiauja su konkurentais dėl saugumo gerinimo ir naudoja iš konkurentų įgytą patirtį, siekdama greičiau išspręsti problemas“. Net 52 įmonės iš 72, ne bendradarbiauja su konkurentais kibernetinio saugumo klausimais. Tai rodo, kad Fintech sektoriaus įmonės nelinkusios dalintis kibernetinių incidentų patirtimi arba nemato poreikio tą daryti.

Kita įdomi tendencija išryškėjusi atlikus tyrimą susijusi su valstybės parama. Net 34 įmonės nesutinka arba negali teigti, jog valstybės parama padeda įmonėms gerinti savo saugumą. Tai galimai rodo, jog arba nėra atitinkamų paramos priemonių siūlomų valstybės lygiu arba įmonės nėra informuotos apie paramos galimybes.

Kitas įdomus tyrimo rezultatas susijęs su kibernetinio saugumo įgūdžiais. Ne visos Fintech įmonės gali teigti, jog turi pakankamai kompetentingų žmogiškųjų išteklių kibernetiniam saugumui užtikrinti. Tik 49 įmonės įvardino, jog turi pakankamai specialistų kibernetiniam

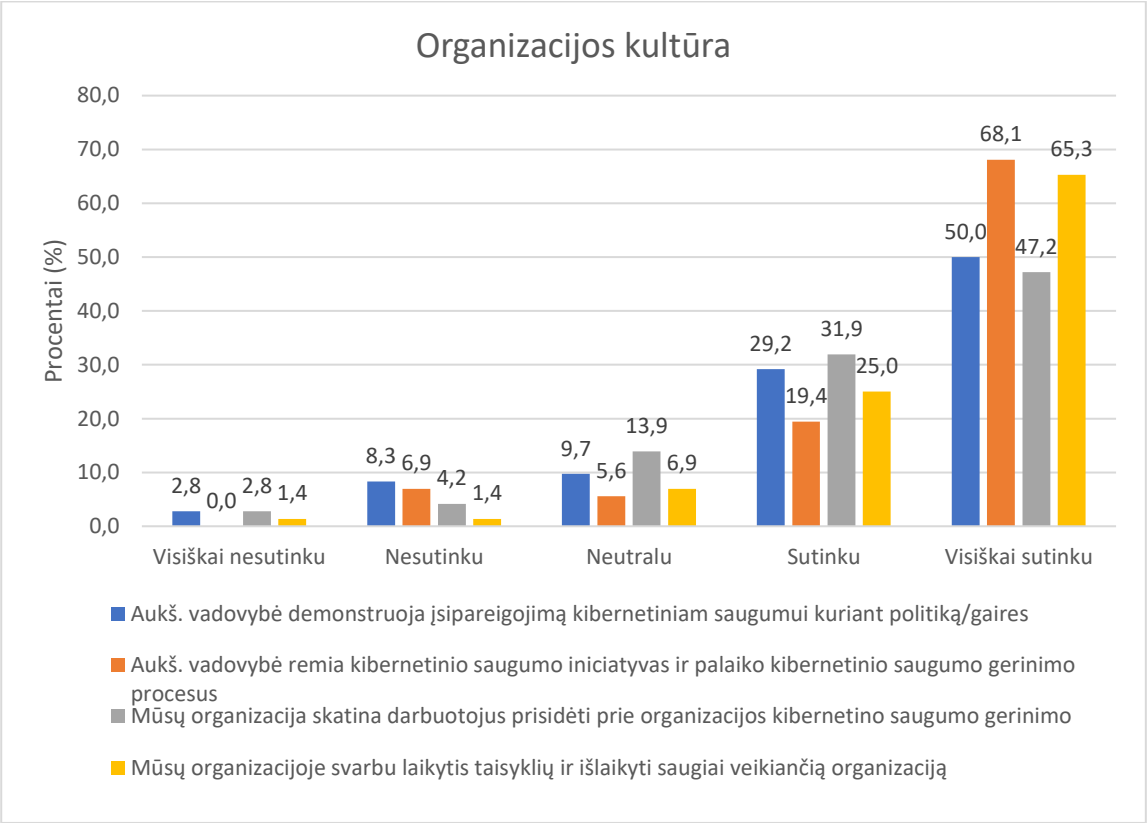
saugumui valdyti bei reguliariai moko savo darbuotojus šia tema, o 47 vertina, jog jų organizacijoje darbuotojai turi pakankamų kibernetinio saugumo įgūdžių.

Toliau dar detaliau aprašomi įvykdyto tyrimo rezultatai.

Rezultatų analizė rodo, kad geriausiai Fintech įmonės Lietuvoje įvertino teiginius susijusius su organizacijos kultūra - aukščiausios vadovybės įsitraukimą į kibernetinį saugumą bei organizacijos kibernetinio saugumo vertybių sklaidą. Atsakymai pateikti paveiksle (žr. **6 paveikslas**).

6 paveikslas

Tyrimo teiginių, apibūdinančių organizacijos kultūrą, rezultatai



Šaltinis: sudaryta autoriaus.

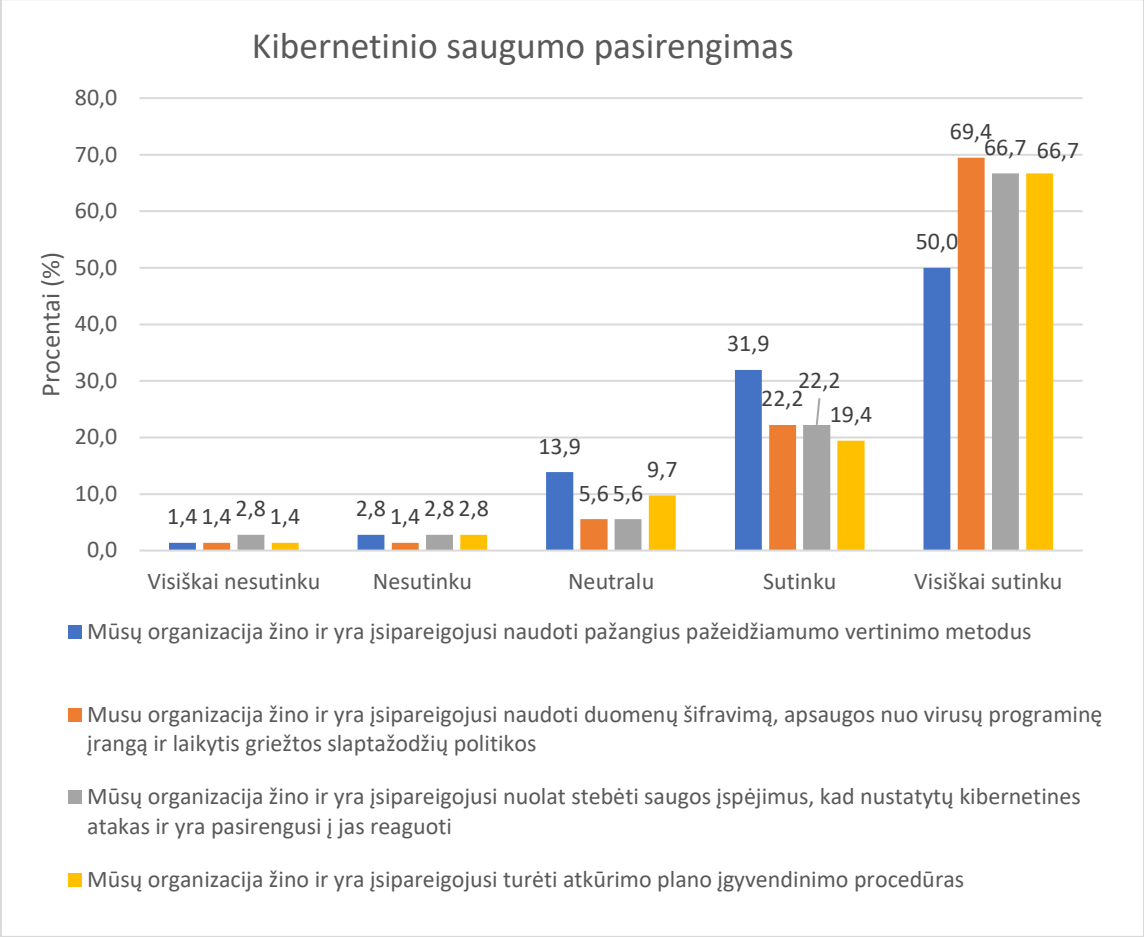
Iš paveikslo duomenų galima matyti, jog 90% tyrime dalyvavusių Fintech įmonių yra svarbu laikytis taisyklių ir išlaikyti saugiai veikiančią organizaciją, o 80% įvardino, jog aukščiausioji vadovybė remia kibernetinio saugumo iniciatyvas ir palaiko kibernetinio saugumo gerinimo procesus. Didelė dalis (79%) pasisakė, jog jų organizacijose kibernetinio saugumo politika/gairės kyla iš aukščiausios vadovybės, tai rodo, jog kibernetinis saugumas užima viena iš strateginių aspektų daugelyje Fintech įmonių Lietuvoje. Taip pat, 79% įmonių skatina savo

darbuotojus prisidėti prie kibernetinio saugumo gerinimo. Daugelis įmonių supranta šių veiksnių svarbą ir jas įgyvendina.

Iš tyrimo rezultatų galima matyti, jog taip pat gerai įvertinti teiginiai, susiję su pasirengimu atremti kibernetines atakas. Fintech įmonės turėjo įvertinti, kaip jos pasirengusios identifikuoti, aptikti kibernetines atakas ir reaguoti į jas bei atsistatyti įvykus incidentui. Rezultatai pateikti paveiksle (žr. **7 paveikslas**).

7 paveikslas

Tyrimo teiginių, apibūdinančių kibernetinio saugumo pasirengimą, rezultatai



Šaltinis: sudaryta autoriaus.

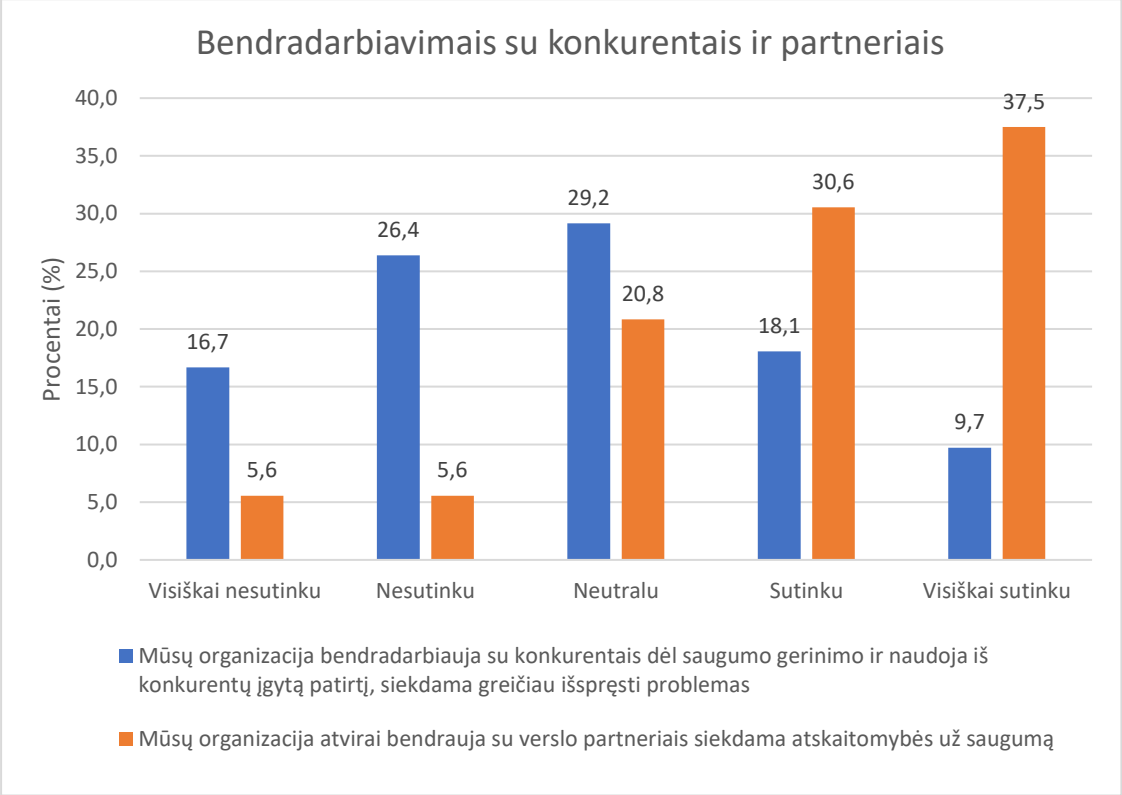
Galima matyti, didžioji dalis respondentų skyrė aukščiausius balus vertindami savo organizacijos kibernetinio saugumo pasirengimą: 92% įmonių naudoja duomenų šifravimą, apsaugos nuo virusu programine įranga ir laikosi griežtos slaptažodžių politikos; 82% nuolat stebi saugos įspėjimus ir yra pasirengusios reaguoti į kibernetines atakas; 86% turi atkūrimo plano įgyvendinimo procedūras. Nors ir didžioji dalis įmonių (82%) naudoja pažangius

pažeidžiamumo vertinimo metodus, galima matyti, jog net 14% respondentų šį teiginį įvertino neutraliai.

Remiantis tyrimo rezultatais, pastebėta, kad prasčiausiai įvertintas išorinis kibernetinio saugumo veiksnys - bendradarbiavimas su konkurentais saugumo gerinimo klausimais. Paveiksle (žr. **8 paveikslas**), pateikti apklausos teiginių, apibūdinančių šį kibernetinio saugumo veiksnį, rezultatai.

8 paveikslas

Tyrimo teiginių, apibūdinančių bendradarbiavimą su konkurentais ir parneriais, rezultatai



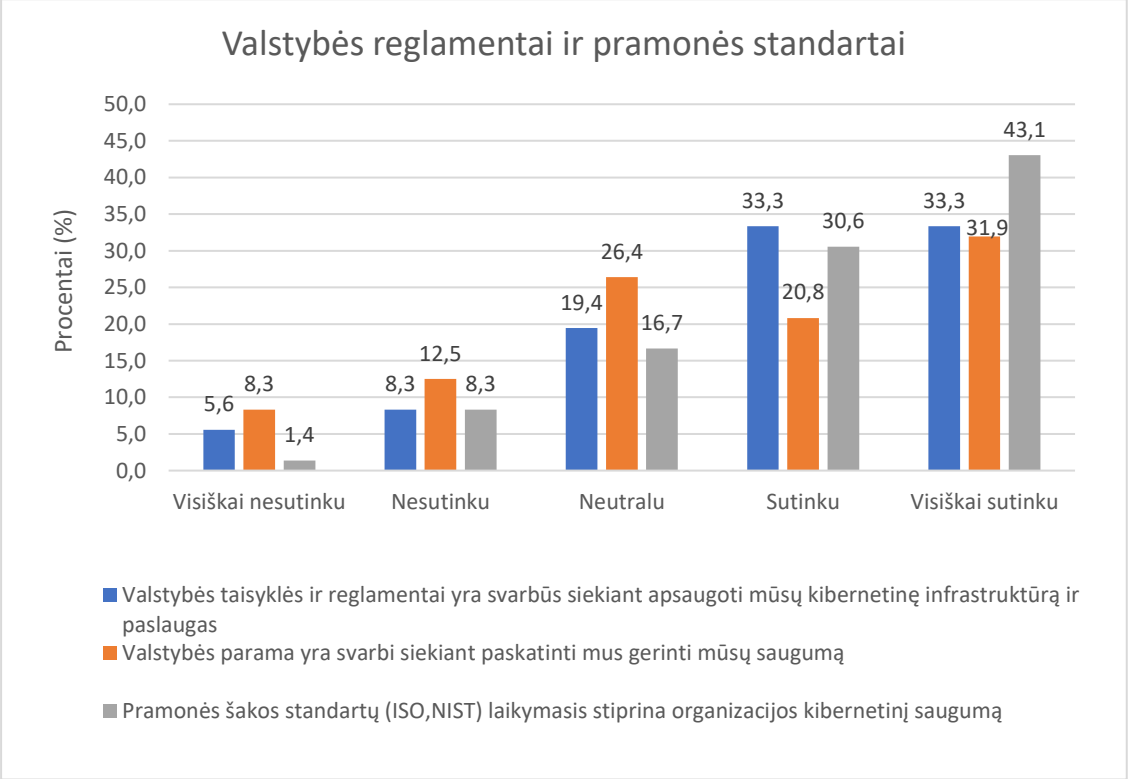
Šaltinis: sudaryta autoriaus.

Tik 28% tyrime dalyvavusių įmonių įvardino bendradarbiaujančios su konkurentais saugumo gerinimo klausimais. Tai rodo, jog Fintech įmonės Lietuvoje įmonės nelinkusios ir didžioji dalis jų nesidalina kibernetinio saugumo klausimais su konkurentais. Taip pat, nenaudoja kitų sukauptos patirties siekdama išspręsti savo saugumo problemas. Daug geresni rezultatai susiję su komunikacija su verslo partneriais – net 68% Fintech įmonių, dalyvavusių tyrime, įvardino, jog bendrauja su verslo partneriais siekdamos atskaitomybės už saugumą. Tai rodo, jog daugumai įmonių svarbu išlikti saugiai veikiančia organizacija ir turėti gerą saugumo statusą bei tuo dalintis su verslo partneriais.

Tyrimo rezultatai parodė, jog taip pat nestipriai Fintech įmonės Lietuvoje įvertino kitą išorinį kibernetinio saugumo veiksnį – valstybės reguliavimą ir paramą. Beveik pusė (47%) dalyvavusių tyrime Fintech įmonių Lietuvoje atstovų įvardino, jog nesutinka arba neturi nuomonės dėl valstybės paramos svarbumo siekiant skatinti įmonių saugumą, bet dauguma (53%) įvardina, jog valstybės reglamentai, taisyklės yra svarbios jų kibernetinio saugumo stiprinimui. Šie rezultatai pateikti paveiksle žemiau (žr. **9 paveikslas**).

9 paveikslas

Tyrimo teiginių, apibūdinančių valstybės reglamentus ir pramonės standartus, rezultatai



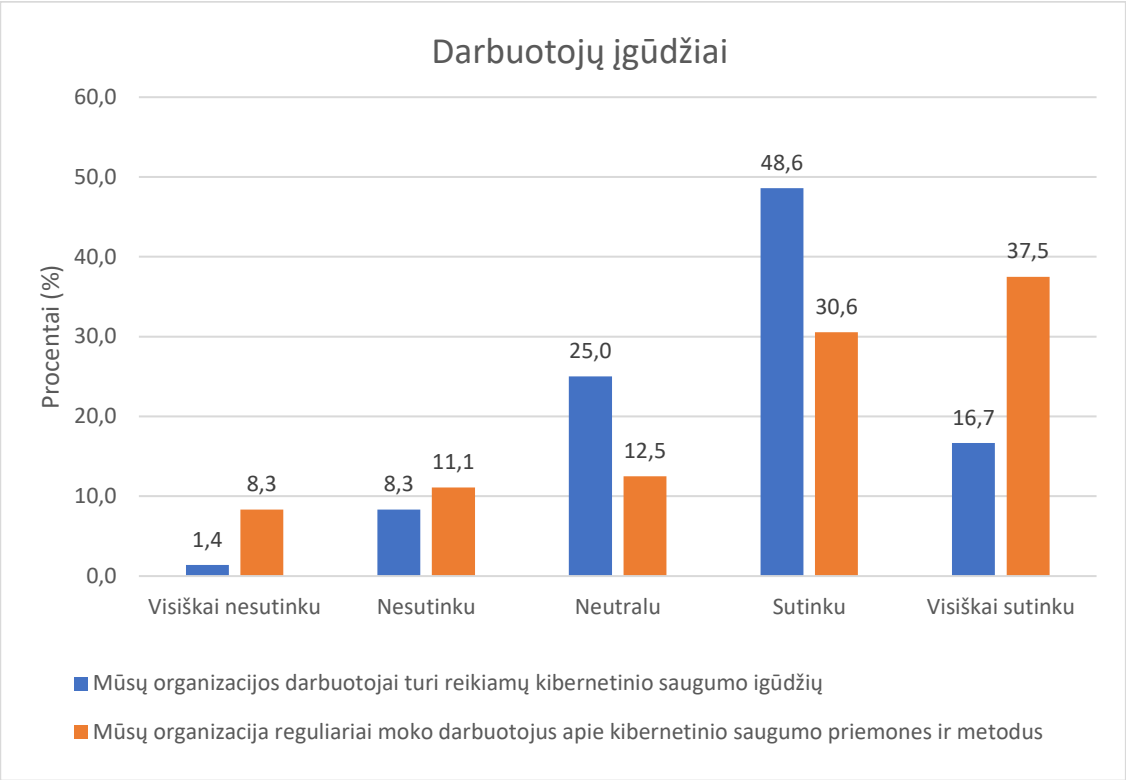
Šaltinis: sudaryta autoriaus.

Iš paveikslo galima matyti, kad geriausiai iš šių teiginių grupės buvo įvertintas standartų (tokių kaip ISO, NIST) laikymasis – 74% Fintech įmonių Lietuvoje sutinka, jog šių standartų laikymasis gerina jų pasirengimą atremti kibernetines atakas ir tai yra svarbus kibernetinio saugumo veiksnys.

Analizuojant tyrimo rezultatus, pastebėta tendencija susijusi su darbuotojų kibernetinio saugumo įgūdžiais. Rezultatai pateikti paveiksle (žr. **10 paveikslas**).

10 paveikslas

Tyrimo teiginių, apibūdinančių darbuotojų įgūdžius, rezultatai



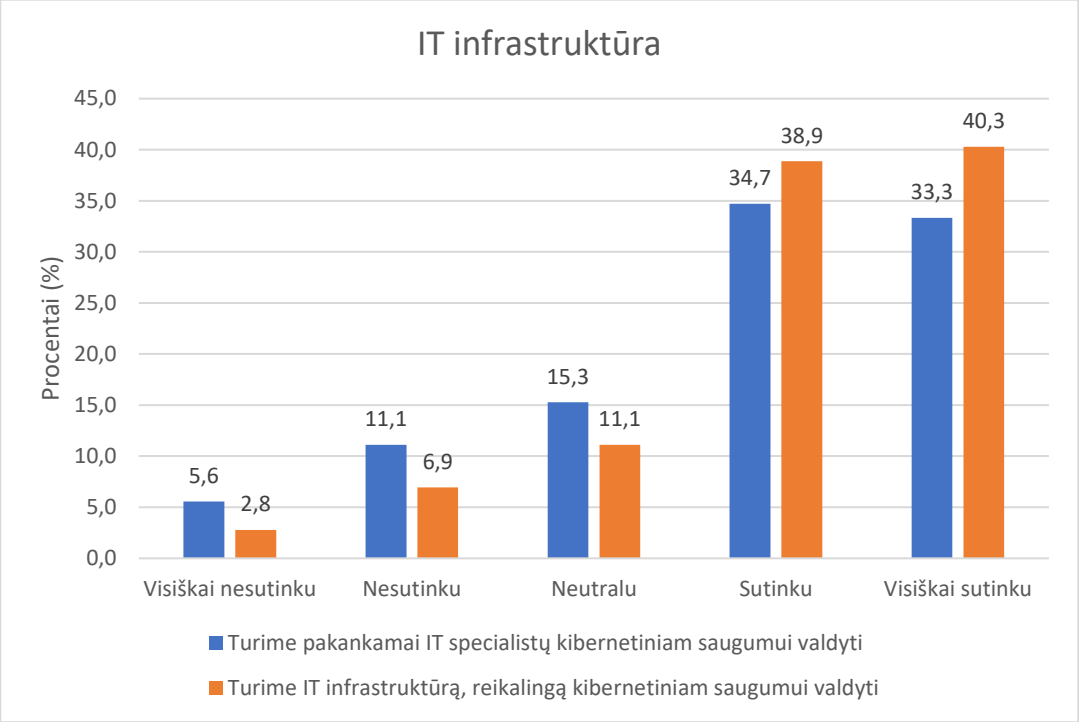
Šaltinis: sudaryta autoriaus.

Nemaža dalis įmonių, net 35%, įžvelgia darbuotojų kibernetinio saugumo įgūdžių trūkumą savo organizacijoje. Taip pat panaši dalis (32%) įmonių patvirtino ir reguliarių mokymų šia tema trūkumą.

Analizuojant atsakymus, susijusius su IT infrastruktūra, reikalinga kibernetiniam saugumui valdyti, galima matyti, jog dauguma Fintech įmonių turi IT infrastruktūrą ir reikalingą specialistų skaičių kibernetiniam saugumui valdyti (žr. **11 paveikslas**).

11 paveikslas

Tyrimo teiginių, apibūdinančių IT infrastruktūrą, rezultatai



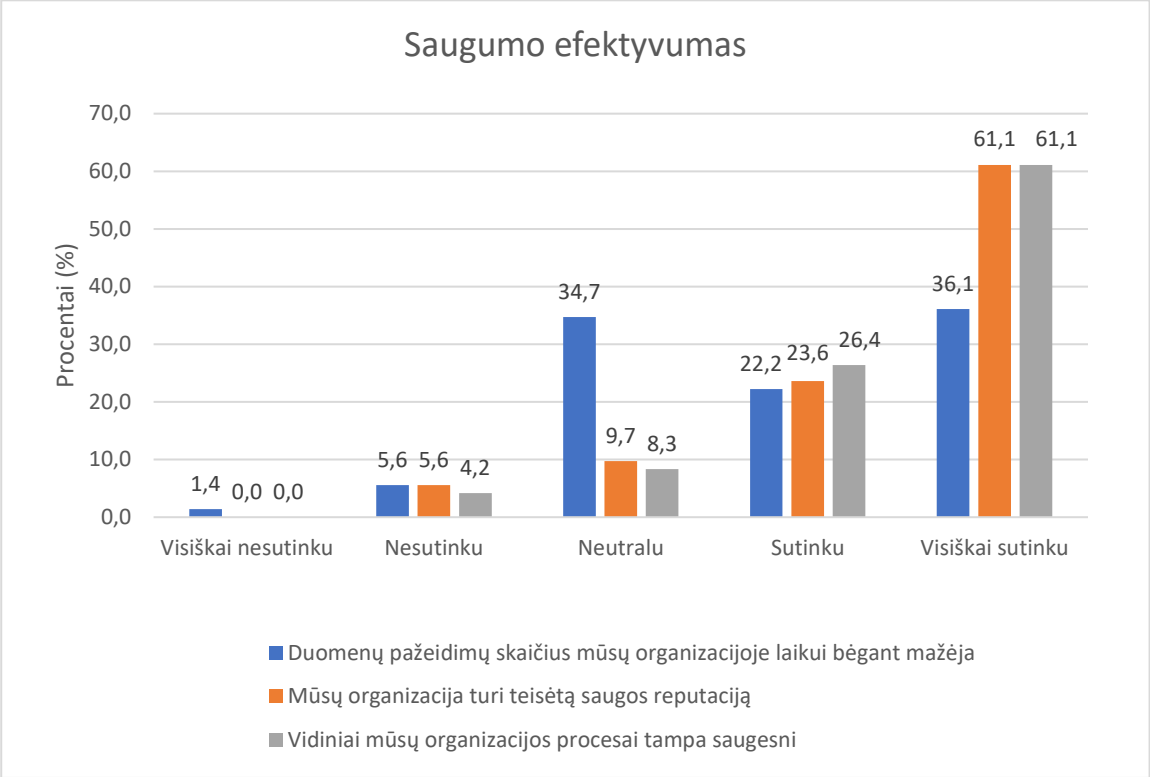
Šaltinis: sudaryta autoriaus.

Nors ir dauguma respondentų gerai vertina savo IT infrastruktūrą, įdomus pastebėjimas, jog net 20% Fintech įmonių negali teigti, jog turi atitinkamą infrastruktūrą kibernetinio saugumo valdymui. Šie tiek daugiau įmonių, 32% vertina, jog neturi reikiamo IT specialistų kiekio kibernetiniam saugumui valdyti arba nemato to poreikio.

Tyrime dalyvavusios Fintech įmonės taip pat turėjo įvertinti ir savo kibernetinio saugumo efektyvumą. 85% įvardino, jog turi teisėtą saugos reputaciją ir 88% Fintech įmonių sutinka, jog procesai jų organizacijose laikui bėgant tampa saugesni. Šie rezultatai pavaizduoti paveiksle žemiau (žr. **12 paveikslas**).

12 paveikslas

Tyrimo teiginių, apibūdinančių saugumo efektyvumą, rezultatai



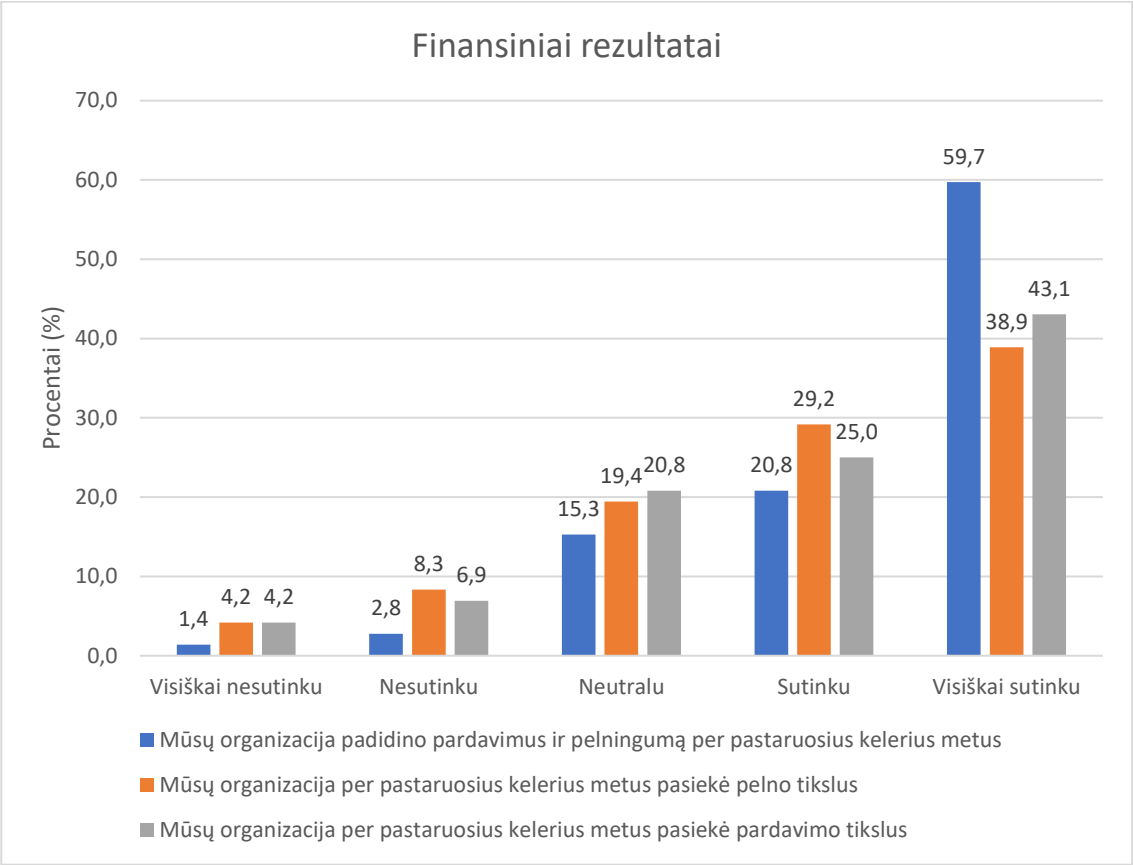
Šaltinis: sudaryta autoriaus.

Iš paveikslo duomenų, galima matyti, kad labai išsiskiria rezultatai susiję su duomenų pažeidimų skaičiumi. Tik daugiau nei pusė (58%) Fintech įmonių Lietuvoje įvardina, jog duomenų pažeidimų skaičius jų organizacijoje laikui bėgant mažėja, nemažai įmonių (35%) šį teiginį įvertino neutraliai, kas gali indikuoti, jog pažeidimų skaičius nekinta arba su jais organizacijos nesusidūrė.

Tyrimo metu respondentai turėjo įvertinti ir savo įmonės veiklos rezultatus. Analizuojant Fintech įmonių veiklos rezultatus apibūdinančius teiginių įvertinimus, pastebėta, jog įmonės per pastaruosius kelerius metus geriau vertina savo nefinansinius rezultatus lyginant su finansiniais rezultatais. Šie rezultatai pateikti paveiksluose žemiau.

13 paveikslas

Tyrimo teiginių, apibūdinančių finansinius rezultatus, įvertinimai



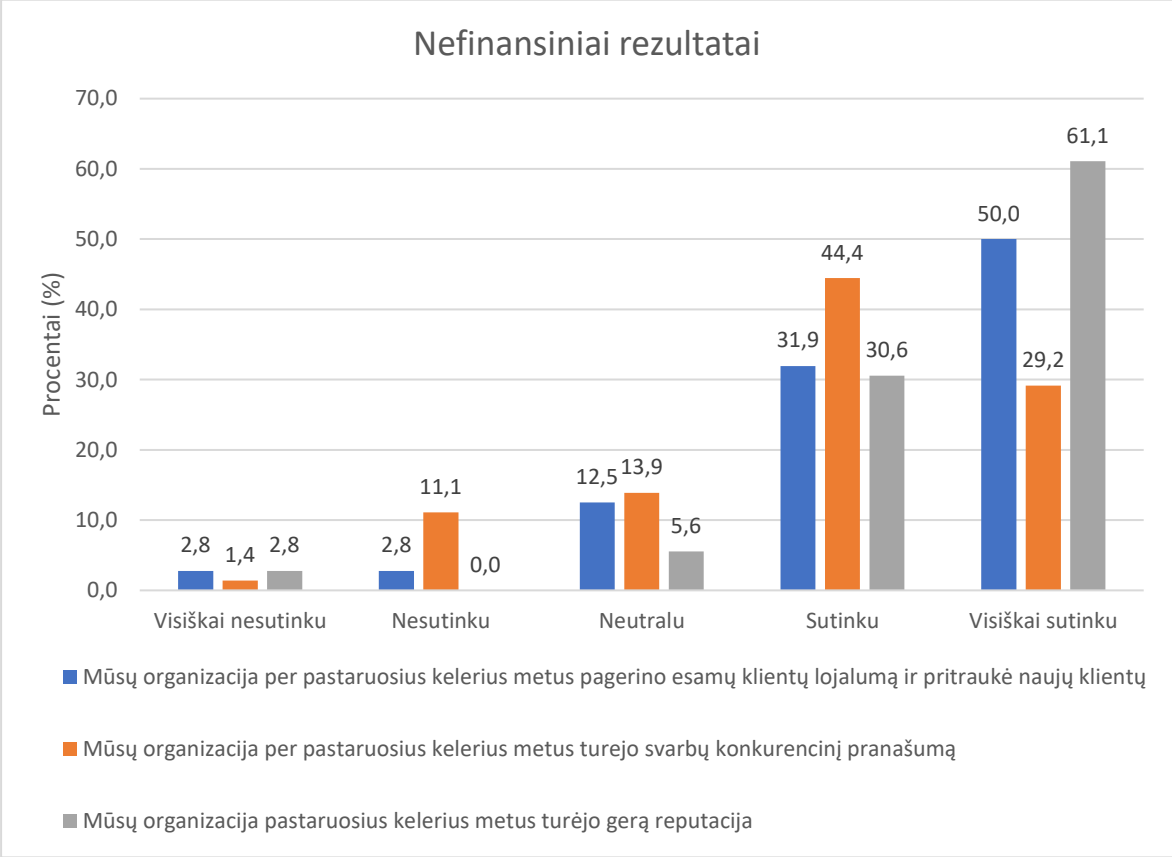
Šaltinis: sudaryta autoriaus.

Iš paveikslo duomenų (žr. **13 paveikslas**) galima pastebėti, kad 81% Fintech įmonių Lietuvoje įvardino, jog per pastaruosius kelerius metus padidino pardavimus ir pelningumą, tačiau tik 68% pasiekė užsibrėžtus pelno ir tiek pat (68%) pardavimų tikslus.

Žemiau paveiksle pavaizduoti nefinansinių rezultatų įvertinimai (žr. **14 paveikslas**)

14 paveikslas

Tyrimo teiginių, apibūdinančių nefinansinius rezultatus, įvertinimai



Šaltinis: sudaryta autoriaus.

Iš pateiktų rezultatų galima, matyti, jog net 82% Fintech įmonių pagerino savo klientų lojalumą ir pritraukė naujų klientų, 74% gali įvardinti, jog turėjo konkurencinį pranašumą ir net 92% įmonių įvardino, kad joms pavyko užtikrinti gerą reputaciją per pastaruosius kelerius metus.

Pagal naudojamą tyrimo modelį šie teiginiai sugrupuoti taip, jog apibūdintų tyrime naudojamus konstruktus. Remiantis šiuo pagrindu, tolimesnei duomenų analizei atlikti buvo sukurti nauji kintamieji. Šie kintamieji apskaičiuoti išvedant visų teiginių įverčių, apibūdinančių konstruktą, vidurkį (sudedami kiekvieno respondento atsakymai į visus teiginius ir suskaičiuojamas vidurkis).

Lentelėje (žr. **9 lentelė**) pateikti tyrimo konstruktų pavadinimai, jų sutrumpinimai (kintamųjų pavadinimai) toliau naudojami analizėje ir pagrindinės statistinės reikšmės.

9 lentelė

Tyrimo konstruktų pagrindinės statistinės vidurkis ir stand. nuokrypis

Tyrimo konstruktai		**Vidurkis**	**Standartinis nuokrypis**
IT Infrastruktūra	IT (IT_1,IT_2)	3,93	1,02
Organizacijos kultūra	OK (OK_1,OK_2,OK_3,OK_4)	4,33	0,81
Darbuotojų įgūdžiai	DI (DI_1,DI_2)	3,74	0,99
Bendradarbiavimas su konkurentais ir partneriais	BKP (BKP_1,BKP_2)	3,33	0,99
Valstybės reglamentai ir pramonės standartai	VRPS ($VRPS_1$, $VRPS_2$,$VRPS_3$)	3,81	0,90
Kibernetinio saugumo pasirengimas	KS (KS_1, KS_2, KS_3, KS_4)	4,44	0,78
Saugumo efektyvumas	S (S_1,S_2,S_3)	4,24	0,78
Finansiniai rezultatai	FR (FR_1, FR_2, FR_3)	4,07	0,98
Nefinansiniai rezultatai	NRF (NFR_1,NFR_2, NFR_3)	4,20	0,80

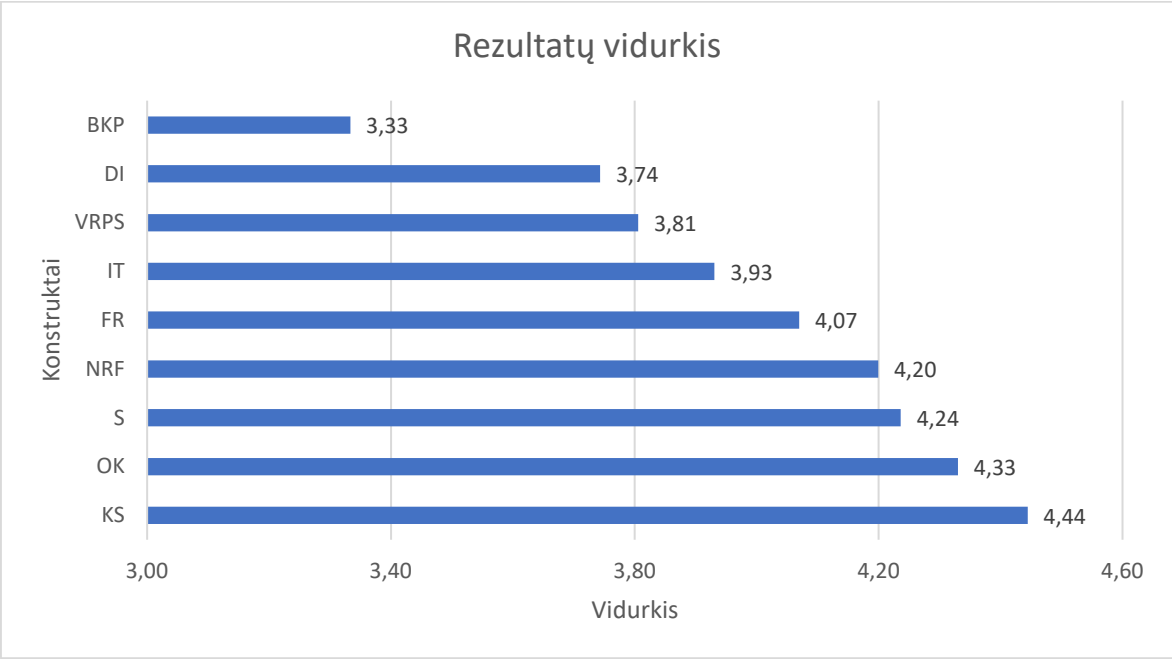
Šaltinis: sudaryta autoriaus.

Iš lentelės duomenų, galima pastebėti, kad standartinio nuokrypio reikšmės visų konstruktų gana panašios. Standartinis nuokrypis parodo kiek daug reikšmės skiriasi nuo vidutinės reikšmės (vidurkio). Didžiausia standartinio nuokrypio reikšmę turi IT infrastruktūros kintamasis, jo reikšmės stipriausiai skiriasi nuo vidutinės reikšmės, lyginant su kitais konstruktais.

Toliau paveiksle pateikti atlikto tyrimo konstruktų įvertinimo rezultatai pagal vidurkį (žr. **15 paveikslas**).

15 paveikslas

Tyrimo konstruktų įvertinimo rezultatai pagal vidurkį



Šaltinis: sudaryta autoriaus.

Iš paveikslo duomenų galima teigti, kad Fintech įmonės Lietuvoje geriausiai įvertino savo kibernetinio saugumo pasirengimą ir organizacijos kultūrą (vienas iš kibernetinio saugumo veiksnių). Taip pat, stipriai vertina savo saugumo efektyvumą bei veiklos rezultatus. Prasčiausiai įvertintas kibernetinio saugumo veiksnys – bendradarbiavimas su konkurentais ir partneriais. IT infrastruktūra Fintech įmonių atstovai įvertino geriau nei darbuotojų įgūdžius ir valstybės reglamentus bei pramonės standartų laikymąsi.

3.2 Koreliacinė ir regresinė analizė

Ryšiui tarp kintamųjų nustatyti buvo atlikta koreliacinė analizė skaičiuojant Spearmano ir Pearsono koreliacijos koeficientus (žr. **10 lentelė**, **11 lentelė**).

Toliau analizės aprašyme naudojami kintamųjų sutrumpinimai, nurodyti anksčiau pateiktoje lentelėje (žr. **9 lentelė**). Detalios koreliacinės analizės lentelės gautos SPSS patektos prieduose (žr. **4 priedas**). Pirmiausia buvo atlikta koreliacinė analizė naudojat Spearmano koreliacijos koeficientą.

10 lentelė

Spearmano koreliacijos koeficientai

		IT	OK	DI	BKP	VRPS	KS	S	FR	NFR
Spearmano koreliacijos koeficientai	IT	1	0,669	0,482	0,382	0,365	0,365	0,334	0,161	0,207
	OK	0,669	1	0,699	0,595	0,350	0,646	0,576	0,261	0,464
	DI	0,482	0,699	1	0,609	0,269	0,574	0,517	0,231	0,379
	BKP	0,382	0,595	0,609	1	0,060	0,512	0,454	0,235	0,217
	VRPS	0,365	0,350	0,269	0,060	1	0,195	0,495	0,325	0,436
	KS	**0,365**	**0,646**	**0,574**	**0,512**	0,195	1	0,633	0,323	0,413
	S	0,334	0,576	0,517	0,454	0,495	0,633	1	**0,392**	**0,539**
	FR	0,161	0,261	0,231	0,235	0,325	0,323	0,392	1	0,630
	NFR	0,207	0,464	0,379	0,217	0,436	0,413	0,539	0,630	1

Šaltinis: sudaryta autoriaus.

Kintamieji statistiškai reikšmingi ir daroma prielaida, kad koreliuoja tarpusavyje jei p (sig.) < 0,05. Atsižvelgiant į tai, galima teigti, kad kintamieji IT,OK, DI, BKP koreliuoja su KS; KS koreliuoja su S; S koreliuoja tiek su FR, tiek su NFR. Spearmano koreliacija rodo, jog koreliacija tarp VRPS ir KS nėra statistiškai reikšminga. Analizei sustiprinti buvo atlikta ir Pearsono koreliacija. Pearsono koreliacijos koeficientai pateikti lentelėje žemiau.

11 lentelė

Pearsono koreliacijos koeficientai

		IT	OK	DI	BKP	VRPS	KS	S	FR	NFR
Pearsono koreliacijos koeficientai	IT	1	0,690	0,552	0,385	0,423	0,540	0,453	0,212	0,304
	OK	0,690	1	0,717	0,600	0,476	0,713	0,712	0,382	0,540
	DI	0,552	0,717	1	0,612	0,281	0,645	0,636	0,367	0,469
	BKP	0,385	0,600	0,612	1	0,139	0,449	0,458	0,282	0,233
	VRPS	0,423	0,476	0,281	0,139	1	0,273	0,503	0,354	0,526
	KS	**0,540**	**0,713**	**0,645**	**0,449**	**0,273**	1	0,754	0,353	0,508
	S	0,453	0,712	0,636	0,458	0,503	0,754	1	**0,447**	**0,589**
	FR	0,212	0,382	0,367	0,282	0,354	0,353	0,447	1	0,739
	NFR	0,304	0,540	0,469	0,233	0,526	0,508	0,589	0,739	1

Šaltinis: sudaryta autoriaus.

Pearsono koreliacija rodo ryšį tarp anksčiau aprašytų kintamųjų, bet taip pat ir rodo statistiškai reikšmingą koreliaciją tarp VRPS ir KS kintamųjų, tačiau ji palyginus labai silpna. Kintamieji koreliuoja vieni su kitais - vyrauja ryšys tarp kibernetinio saugumo veiksnių tarpusavyje. Taip pat, tarp FR ir NFR bei S kintamųjų. Visi lentelėse pateikti koreliacijos koeficientai teigiami, tai rodo, jog vyrauja tik tiesioginis ryšys tarp kintamųjų, tiesioginė priklausomybė, t.y. vieno kintamojo reikšmei didėjant, atitinkamai didėja ir kito kintamojo reikšmės. Stipriausias ryšis iš kibernetinio saugumo veiksnių yra tarp OK ir KS; DI ir KS; Šiek tiek silpniau koreliuoja BKP ir KS; IT ir KS. Gana stipriai koreliuoja OK ir DI bei KS ir S. S koreliuoja tiek su FR, tiek su NFR, tačiau stipresnis ryšys yra su NFR. S koreliuoja su visais kibernetinio saugumo veiksniais, stipriausias ryšys su OK, DI, VRPS, BKP.

Remiantis tuo, jog ryšys tarp kintamųjų rastas, toliau atliekama daugianarė tiesinė regresinė analizė. Šia analize siekiama išsiaiškinti ar nuo nepriklausomų kintamųjų priklauso ir

priklausomo kintamojo reikšmės, ieškomi priežastiniai ryšiai tarp kintamųjų. Taip pat siekiama patikrinti iškeltas tyrimo hipotezes.

Pirmiausia buvo atliekama tiesinė regresinė analizė siekiant išsiaiškinti, kokie veiksniai turi įtakos kibernetinio saugumo pasirengimui. KS – priklausomas kintamasis; IT, OK, DI, BKP, VRPS – nepriklausomi kintamieji. Regresinės analizės rezultatai pateikti lentelėje (žr. **12 lentelė**). Išsamūs regresinės analizės rezultatai gauti SPSS pateikti prieduose (žr. **5 priedas**).

Atliekant regresinę analizę, buvo atsižvelgta į gauto modelio tinkamumą. Determinacijos koeficiento reikšmė didesnė už 0,20 (R2 = 0,553), todėl daroma prielaida, kad modelis tinkamas.

Toliau buvo patikrintos ANOVA reikšmės. ANOVA reikšmė mažesnė net už 0,001, todėl daroma išvada, jog modelyje yra bent vienas kintamasis – regresorius, nuo kurio priklauso KS (kibernetinio saugumo pasirengimas).

Stulpelyje p-reikšmė yra nurodytos Stjudento kriterijaus p reikšmės, jei $p < 0,05$, daroma išvada, jog regresorius yra statistiškai reikšmingas. Tuo remiantis, galima teigti, kad regresoriai OK ir DI yra statistiškai reikšmingi, o regresoriai IT, BKP ir VRPS statistiškai nereikšmingi šiame modelyje. Taip pat, VIF <4, tai rodo, jog multikolinearumo tarp kintamųjų problemos modelyje nėra.

Nestandartizuotas beta koeficiento ženklai parodo ar didėjant regresoriams, didės ar mažės priklausomas kintamasis. Jei šio koeficiento reikšmės mažesnės už 0, tai regresoriui didėjant, priklausomas kintamasis mažėja ir , atvirkščiai, jei koeficiento reikšmės didesnės už 0 - tai regresoriui didėjant, priklausomas kintamasis irgi didėja.

Standartizuotas beta koeficientas parodo regresoriaus įtaką priklausomam kintamajam. Kuo standartizuotas beta koeficientas didesnis, tuo atitinkamo regresoriaus įtaka modelyje didesnė.

Iš gautų rezultatų galime matyti, jog abiejų statistiškai reikšmingų regresorių nestandartizuoto beta koeficiento reikšmės teigiamos, o didžiausią įtaką kibernetinio saugumo pasirengimui turi OK, nes standartizuoto beta koeficiento reikšmės didžiausios.

12 lentelė

Tiesinės regresinės analizės rezultatai (1)

Hipotezė	Nestand. Beta koef.	Stand. Beta koef.	R2	F	t-reikšmė	p-reikšmė	VIF	Hipotezė patvirtinta
H1: IT → KS	0,056	0,073	0,553	16,347	0,626	0,534	1,995	NE
H2: OK → KS	0,518	0,539	0,553	16,347	3,544	<0,001	3,418	TAIP
H3: DI→ KS	0,221	0,281	0,553	16,347	2,225	0,029	2,351	TAIP
H4: BKP→ KS	-0,049	-0,063	0,553	16,347	-0,565	0,574	1,818	NE
H5: VRPS → KS	-0,073	-0,085	0,553	16,347	-0,874	0,385	1,383	NE

Šaltinis: sudaryta autoriaus.

Išsiaiškinus kibernetinio saugumo pasirengimo regresorius buvo atliekama regresinė analizė patikrinti likusias hipotezes. Buvo ieškoma ar kibernetinio saugumo pasirengimas turi įtakos saugumo efektyvumui (KS – nepriklausomas kintamasis, S – priklausomas kintamasis). Taip pat ar saugumo efektyvumas turi įtakos finansiniams ir nefinansiniams rezultatams (S-nepriklausomas, NR – priklausomas kintamasis; S - nepriklausomas kintamasis, NFR – priklausomas). Gauti rezultatai pateikti lentelėje (žr. **13 lentelė**). Išsamūs regresinės analizės rezultatai gauti SPSS pateikti prieduose (žr. **6 priedas**, **7 priedas**, **8 priedas**).

Atliktų tiesinių regresinių analizių determinacijos koeficiento reikšmės užtikrina modelių tinkamumą. ANOVA reikšmės mažesnė net už 0,001, todėl daroma išvada, jog visuose modeliuose yra kintamasis – regresorius, nuo kurio priklauso S, FR ar atitinkamai, NFR.

Be to, iš gautų rezultatų galime matyti, kad visų statistiškai reikšmingų regresorių nestandartizuoto beta koeficiento reikšmės teigiamos, tai rodo, jog šiems regresoriams didėjant, didėja ir priklausomo kintamojo reikšmės.

13 lentelė

Tiesinės regresinės analizės rezultatai (2)

Hipotezė	Nestand. Beta koef.	Stand. Beta koef.	R2	F	t-reikšmė	p-reikšmė	Hipotezė patvirtinta
H6: KS → S	0,760	0,754	0,568	91,981	9,591	<0,001	TAIP
H7 S → FR	0,558	0,447	0,200	17,450	4,177	<0,001	TAIP
H8: S → NFR	0,605	0,099	0,347	37,278	6,106	<0,001	TAIP

Šaltinis: sudaryta autoriaus.

Apibendrinus rezultatus, atliktos koreliacinės analizės metu rastas stiprus tiesioginis ryšys tarp Fintech įmonių Lietuvoje kibernetinio saugumo pasirengimo ir organizacijos kultūros bei darbuotojų įgūdžių. IT infrastruktūra bei bendradarbiavimas su konkurentais ir partneriais taip pat turi ryšį su kibernetinio saugumo pasirengimu, tačiau ryšys tarp jų silpnesnis. Išsiaiškinta, jog Fintech įmonių saugumo efektyvumas labai priklauso nuo įmonių kibernetinio saugumo pasirengimo ir turi tiesioginį ryšį ir su kibernetinio saugumo veiksniais – organizacijos kultūra, darbuotojų įgūdžiais, valstybės reglamentų ir pramonės standartų laikymųsi, bendravimu su partneriais ir konkurentais kibernetinio saugumo tema bei IT infrastruktūra. Taip pat rastas labai stiprus tiesioginis ryšys tarp Fintech įmonių Lietuvoje kibernetinio pasirengimo ir saugumo efektyvumo. Saugumo efektyvumas tiesiogiai koreliuoja su Fintech įmonių finansiniais, o labiausiai su nefinansiniais veiklos rezultatais.

Regresinės analizės metu atmestos H1, H4, H5 hipotezės, nes kintamieji IT infrastruktūra (IT), bendradarbiavimas su partneriais ir konkurentais (BKP), valstybės reglamentai ir pramonės standartai (VRPS) nebuvo statistiškai reikšmingi modelyje.

Regresinės analizės metu priimtos H2, H3, H6, H7, H8 hipotezės:

- Nustatyta, jog Fintech įmonių Lietuvoje kibernetinio saugumo pasirengimo statistiškai reikšmingi regresoriai yra organizacijos kultūra ir darbuotojų įgūdžiai. Stipriausiai kibernetinio saugumo pasirengimą veikia organizacijos kultūra.
- Nustatyta, kad kibernetinio saugumo pasirengimas turi įtakos organizacijos kibernetinio saugumo efektyvumui.

- Nustatyta, jog Fintech įmonių kibernetinio saugumo efektyvumas turi įtakos finansiniams rezultatams ir nefinansiniams rezultatams. Nustatyta, jog tarp finansinių ir nefinansinių rezultatų yra stiprus tiesioginis ryšys.

IŠVADOS

1. Kibernetinė rizika yra įvardijama bet kokia rizika, susijusi su finansiniais nuostoliais, veiklos sutrikdymu ar organizacijos reputacijos sugadinimu dėl įvykio, turinčio įtakos organizacijos informacijai ir (arba) informacinėms sistemoms. Kibernetiniai incidentai klasifikuojami į duomenų konfidencialumo pažeidimus; sistemos gedimą, problemą; duomenų prieinamumą ir kenkėjiška veiklą.
2. Kibernetinis saugumas yra visuma priemonių, naudojamų apsaugoti kibernetinę aplinką ir užtikrinti informacinėmis sistemomis perduodamą ar jose tvarkomą elektroninę informaciją. Pagrindinis kibernetinio saugumo aspektas yra užtikrinti informacijos konfidencialumą, prieinamumą ir vientisumą.
3. Remiantis atlikta mokslinių šaltinių analize, įmonės pasirengimą atremti kibernetines atakas gerina technologiniai, organizaciniai ir aplinkos veiksniai. Technologinius veiksnius sudaro IT infrastruktūra ir ištekliai ją valdyti. Organizaciniai veiksniai yra aukščiausios vadovybės įsitraukimas, organizacijos kultūra ir darbuotojų įgūdžiai. Aplinkos veiksnius sudaro valstybės reglamentai ir parama, pramonės šakos standartų laikymasis bei bendradarbiavimas su partneriais ir konkurentais kibernetinio saugumo tema.
4. Remiantis atlikta mokslinių šaltinių analize, kibernetiniai incidentai gali turėti didelę neigiamą reikšmę įmonės veiklos rezultatams – veiklos procesų tęstinumui, konkurencingumui, reputacijai, finansiniams rezultatams. Geras pasirengimas atremti kibernetines atakas stiprina įmonės kibernetinio saugumo efektyvumą, o šis teigiamai veikia įmonės finansinius ir nefinansinius rezultatus.
5. Įvairių sektorių įmonės nepriklausomai nuo dydžio gali tapti kibernetinių išpuolių aukomis, tačiau labiausiai kibernetinių atakų veikiami yra viešasis ir finansų sektoriai dėl ypatingos svarbos informacinių išteklių. Finansinių technologijų sektoriaus įmonės yra svarbi finansų ekosistemos dalis, nes siūlo technologijomis grįstus finansiniu produktus ir paslaugas, tačiau taip pat yra ir kibernetinių atakų taikinys.
6. Atlikto tyrimo rezultatai patvirtino, jog geresnis kibernetinio saugumo pasirengimas, kuris pasiekiamas stiprinant organizacijos kultūrą ir darbuotojų įgūdžius, didina įmonių kibernetinio saugumo efektyvumą. Šis rezultatas patvirtina anksčiau atliktų tyrimų rezultatus.

7. Remiantis tyrimu, galima teigti, jog kibernetinis saugumas turi įtakos įmonės finansiniams ir nefinansiniams veiklos rezultatams Fintech sektoriaus įmonėse Lietuvoje. Įmonės stiprindamos kibernetinio saugumo veiksnius gali pasiekti geresnių veiklos rezultatų – didinti pardavimus ir pelną, pritraukti naujus klientus ir išlaikyti jų lojalumą. Taip pat geresnis kibernetinio saugumo pasirengimas stiprina konkurencinį pranašumą ir įmonių reputaciją. Šis rezultatas patvirtina anksčiau atliktų tyrimų rezultatus.
8. Tyrimo rezultatai patvirtino didelę organizacijos kultūros įtaką Fintech įmonių Lietuvoje pasirengimui kovoti su kibernetinėmis atakomis. Šis rezultatas patvirtina anksčiau atliktų tyrimų rezultatus. Remiantis tyrimo rezultatais įmonės stipriai vertina ir supranta šio kibernetinio saugumo veiksnio svarbą ir skiria nemažai dėmesio kultūros kibernetinio saugumo atžvilgiu vystymui organizacijose. Aukščiausioji vadovybė Fintech įmonėse ne tik įsitraukus į kibernetinio saugumo iniciatyvas, bet ir skatina išlaikyti saugiai veikiančios organizacijos statusą.
9. Tyrimo rezultatai patvirtino didelę darbuotojų įgūdžių įtaką Fintech įmonių Lietuvoje pasirengimui kovoti su kibernetinėmis atakomis. Šis rezultatas patvirtina anksčiau atliktų tyrimų rezultatus. Remiantis tyrimo rezultatais, dalis įmonių susiduria su darbuotojų ir kompetencijos trūkumų reikiamų valdyti kibernetinį saugumą.
10. Tyrimo rezultatai parodė, jog egzistuoja ryšys tarp bendradarbiavimo su partneriais ir konkurentais, ir kibernetinio saugumo pasirengimo. Tačiau šio veiksnio įtaką Fintech įmonėse Lietuvoje kibernetinio saugumo pasirengimui nenustatyta. Šis rezultatas skiriasi nuo anksčiau atliktų tyrimų rezultatų.
11. Tyrimo rezultatai parodė, jog egzistuoja ryšys tarp valstybės reguliavimo bei pramonės standartų laikymosi ir kibernetinio saugumo pasirengimo. Tačiau šio veiksnio įtaką Fintech įmonių Lietuvoje kibernetinio saugumo pasirengimui nenustatyta. Rezultatas skiriasi nuo anksčiau atliktų tyrimų rezultatų. Fintech įmonės Lietuvoje vertina valstybės reglamentų laikymąsi kaip svarbų veiksnį, tačiau žymaus valstybės reglamentų ir paramos poveikio saugumui nepastebi. Tyrimo rezultatai rodo, jog saugumo standartų laikymąsi Fintech įmonės suvokia kaip svarbų kibernetinio saugumo stiprinimo veiksnį.
12. Tyrimo rezultatai parodė, jog egzistuoja ryšys IT infrastruktūros, reikalingos kibernetiniam saugumui valdyti, ir kibernetinio saugumo pasirengimo. Tačiau šio

veiksnio įtaką Fintech įmonių Lietuvoje kibernetinio saugumo pasirengimui nenustatyta. Šis rezultatas skiriasi nuo anksčiau atliktų tyrimų rezultatų. Net ir turint gerą IT infrastruktūrą ir pakankamą darbuotojų skaičių kibernetinio saugumo valdymui, svarbiau yra šių išteklių panaudojimas. Galima daryti išvadą, jog tik turėti nepakanka – reikia investuoti į darbuotojų kompetenciją bei kurti organizacijos kultūrą, kuri skatintų tinkamai taikyti turimą IT infrastruktūrą kibernetinei rizikai valdyti.

REKOMENDACIJOS

1. Įmonės siekdamos pagerinti savo finansinius bei nefinansinius rezultatus turėtų atitinkamai dėmesio skirti kibernetinio saugumo veiksnių, ypač organizacinių – organizacijos kultūros ir darbuotojų įgūdžių, stiprinimui. Kibernetinio saugumo veiksniai gerina organizacijos kibernetinį saugumą, kuris teigiamai veikia tiek įmonės reputaciją, konkurencingumą bei klientų lojalumą ir pritraukimą. Šie nefinansiniai rezultatai taip pat yra gerų ilgalaikių finansinių rezultatų pagrindas.
2. Siekiant padidinti organizacijų pasirengimą kovoti su kibernetinėmis atakomis, kuriant kibernetinį saugumą siūloma įmonėse skatinti organizacijos kultūrą, kuri susideda iš aukščiausio lygio vadovų įsitraukimo kuriat kibernetinio saugumo politiką, strategijas, gaires, taisykles ir standartus bei kibernetinio saugumo vertybių sklaidos įmonėje. Aukščiausio lygio vadovai turėtų rodyti atsakingumą kibernetinio saugumo klausimais asmeniškai įsitraukdami į su kibernetinio saugumu susijusius klausimus, įsipareigoti remti kibernetinio saugumo iniciatyvas ir gerinimo procesus. Siūloma, jog aukščiausioji vadovybė turėtų suformuluotą viziją įmonės kibernetinio saugumo gerinimui. Organizacijos kultūros gerinimui taip pat siūloma skatinti darbuotojų įsitraukimą į kibernetinio saugumo gerinimą ir kurti organizacijos kultūrą, kurioje svarbu laikytis taisyklių, bendradarbiauti ir išlaikyti saugiai veikiančią įmonę.
3. Siūloma įmonėms skirti pakankamai dėmesio darbuotojų kibernetinio saugumo įgūdžių gerinimui siekiant stiprinti organizacijos kibernetinį saugumą. Darbuotojų kibernetinio saugumo įgūdžiai ir kompetencijos gali būti lavinami reguliariai organizuojant darbuotojų mokymus bei suteikiant prieigą prie reikiamų išteklių, kurie sustiprintų mokymosi procesą. Siūloma gerinti darbuotojų įgūdžius, nes tai prisidės prie efektyvesnių IT infrastruktūros panaudojimo galimybių siekiant apsaugoti įmones nuo kibernetinės rizikos.
4. Siekiant gerinti kibernetinį saugumą taip pat siūloma stiprinti bendradarbiavimą su konkurentais ir partneriais kibernetinio saugumo tema. Nors tyrimo metu nepavyko rasti šio veiksnio įtakos kibernetinio saugumo pasirengimui, tačiau ankstesni tyrimai rodo teigiamą šio veiksnio įtaką. Įmonės nelinkusios dalintis informacija su konkurentais galimai dėl nepasitikėjimo ir baimės, kad informacija susijusi su kibernetiniais incidentais ar priemonėmis gali būti panaudota prieš juos, taip pat, Fintech įmonės Lietuvoje galimai vengia dalytis su saugumu

susijusia patirtimi, įžvalgomis ir įgūdžiais, kad įgytų saugumo pranašumą prieš konkurentus arba nemato galimybės, kur galėtų dalintis savo patirtimi. Siūloma Fintech įmones vienijančias organizacijas, tokias kaip „Fintech Lietuvoje“ ar „Rockit“ kurti kibernetinio saugumo praktikų dalijimosi bendruomenę, kurioje savanoriškai būtų galima dalintis savo patirtimi.

5. Siekiant gerinti Fintech įmonių kibernetinį pasirengimą valstybės lygiu, turėtų būti atitinkamai skiriama daugiau dėmesio įgyvendinant paramą ir reguliavimą kibernetinio saugumo klausimu. Valstybė turėtų teikti vertingesnę paramą ir pagalbą – galėtų būti organizuojamos įvairios kibernetinio saugumo iniciatyvos (pvz., seminarai) bei stiprinimas jų žinomumas. Tai išryškintų valstybės reguliavimo ir paramos naudą Fintech sektoriaus ir kitų įmonių atžvilgiu.
6. Siūloma taikyti ir laikytis saugumo standartų (pvz., NIST, ISO), kurie padėtų kovoti su kibernetinėmis atakomis ir stiprintų kibernetinį pasirengimą. Standartų gairių ir gerųjų praktikų taikymas turėtų padėti organizacijoms sumažinti kibernetinio saugumo incidentų ir neigiamų jų pasekmių poveikį, tačiau tinkamam šių standartų taikymui reikėtų jų specifiką Lietuvoje adaptuoti remiantis teisine, ekonomine aplinka. Atitinkamai ir mažoms įmonėms siūloma atsirinkti ir naudoti saugumo standartų gerąsias praktikas.

LITERATŪROS SĄRAŠAS

A.V.Skrypnikov, Kozlov, V., Denisenko, V. V., A.Saranov, I., Kuznecova, E. D., & Savchenko, I. I. (2020). Information Security as the Basis of Digital Economy. *Advances in Economics, Business and Management Research*, 149-153.

Adeyoju, A. (2019). *Cybercrime and Cybersecurity: FinTech's Greatest Challenges.* University of Saskatchewan.

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability 60, 100989*.

Ali, L. (2019). Cyber crimes-A constant threat for the business sectors and its growth (A study of the online banking sectors in GCC). *The Journal of Developing Areas 53, no. 1* .

Allen, F., Gu, X., & Jagtiani, J. (2020). *A survey of fintech research and policy discussion.*

Angst, C. M., Block, E. S., Block, J. D., & Kelley, K. (2016). When do IT security investments matter? . *Accounting for the Influence of Institutional Facto in the context of healthcare data breaches.*

Antoine, B. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment.* International Monetary Fund.

Basel Committee on Banking Supervision. (2001). *The Regulatory Treatment of Operational Risk, Working Paper*. Nuskaityta iš http://www.bis.org/publ/bcbs_wp8.pdf

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance, 28*, 24-31.

Benson, V. (2017). *The state of global cyber security: Highlights and key findings.* London. doi:10.13140/RG.2.2.22825.49761

Bilevičienė, T., & Jonušauskas, S. (2011). *Statistinių metodų taikymas rinkos tyrimuose.* MRU.

Blazevic, V., & Lievens, A. (2004). Learning during the new financial service innovation process: antecedents and performance effects. *Journal of business research 57, no. 4*, 374-391.

Bouncken, R. B., & Fredrich, V. (2016). Learning in coopetition: Alliance orientation, network size, and firm types. *Journal of Business Research 69, no. 5*, 1753-1758.

Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment.* International Monetary Fund.

Callen-Naviglia, J., & James, J. (2018). FINTECH, REGTECH AND THE IMPORTANCE OF CYBERSECURITY. *Issues in Information Systems 19, no. 3*, 220-225. doi:https://doi.org/10.48009/3_iis_2018_220-225

Canongia, C., & Mandarino, R. (2012). Cybersecurity: The new challenge of the information society. *Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions*, 165-184.

Cebula, J. J., & Young, L. R. (2010). *A taxonomy of operational cyber security risks.* Pittsburgh: Carnegie-Mellon University Software Engineering Institure. Nuskaityta iš https://apps.dtic.mil/sti/pdfs/ADA537111.pdf

Chang, S. E., & Bruce Ho. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems* .

Clarke, R. A., & Knake, R. K. (2014). *Cyber war. The Next Threat to National Security and What to Do About It.* Old Saybrook: Tantor Media, Incorporated.

Committee on National Security Systems. (2015 m. 04 6 d.). Committee on National Security Systems (CNSS) Glossary No. 4009. Paimta 2021 m. 12 24 d. iš https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

Copeland, M. (2017). Cybersecurity: How security vulnerabilities affect your business. *Cyber Security on Azure. Apress, Berkeley, CA*, 3-31.

Čekanavičius, V., & Murauskas, G. (2014). *Taikomoji regresinė analizė socialiniuose tyrimuose.* Vilniaus universiteto leidykla.

D'Arcy, J., Herath, T., & K. Shoss, M. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of management information systems 31, no. 2*, 285-318.

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations? *International Journal of Business & Society 19, no. 1*.

Eccles, R. G., Ioannou, l., & Serafeim, G. (2014). The impact of corporate sustainability on organizational processes and performance. *Management science 60, no. 11*, 2835-2857.

Eilts, D. (2020). *An empirical assessment of cybersecurity readiness and resilience in small businesses.*

Eling, M., & Schnell, W. (2017). Ten key questions on cyber risk and cyber risk insurance. *Asia Insurance Review 1*. Nuskaityta iš https://www.alexandria.unisg.ch/259959/

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research 272, no. 3*, 1109-1119.

Elnagdy, S. A., Qiu, M., & Gai, K. (2016). Cyber incident classifications using ontology-based knowledge representation for cybersecurity insurance in financial industry. *In 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing*, (p. 301-306).

Faya, M., & Ogbuefi, N. (2019). Cybersecurity in the Age of FinTech and Digital Business. *In Cyber Secure Nigeria 2019 Conference.*

Garvin, D. A. (1998). The processes of organization and management. *Sloan Management Review, 39(4)*, 33-51.

Gopal, A., & Gosain, S. (2010). Research note—The role of organizational controls and boundary spanning in software development outsourcing: Implications for project performance. *Information systems research 21, no. 4*, 960-982.

Grincevičius, R. (2019). *Kibernetinio saugumo valdymo gerinimas taikant atsparumo modelius organizacijose.* MRU.

Hasan, S., Ali, M., & Kurnia, S. T. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications (58)*. doi:https://doi.org/10.1016/j.jisa.2020.102726

Hernandez, S., & Schou, C. (2014). *Information Assurance Handbook: Effective Computer Security and Risk Management Strategies.* McGraw-Hill Education Group.

Héroux, S., & Fortin, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives 19, no. 2*, 73-100.

Hsu, C., Lee, J.-N., & W. Straub, D. (2012). Institutional Influences on Information Systems Security Innovations. *Information Systems Research 23*. doi:https://doi.org/10.1287/isre.1110.0393

Iivari, J., & Huisman, M. (2007). The relationship between organizational culture and the deployment of systems development methodologies. *Mis Quarterly*, 35-58.

Invest Lithuania. (2022). *The Fintech Landscape in Lithuania, 2021-2022 Report.*

IRM. (2018). *Cyber Risk. Resources for Practitioners.* The Institute of Risk Management. Nuskaityta iš https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf

ISACA. (2009). *The Risk IT Framework.* Nuskaityta iš https://www.hci-itil.com/ITIL_v3/docs/RiskIT_FW_30June2010_Research.pdf

James, L. (2018). Making cyber-security a strategic business priority. *Network Security*, 6-8.

Janeliūnienė, R., & Davidavičienė, V. (2013). IT rizikos identifikavimo proceso analizė. *Science - future of Lithuania, (5.1)*, 46-52.

Jevsejev, R. (2020). Informacinių technologijų rizikos vertinimo metodai ir tobulinimo sprendimai. *Mokslas - Lietuvos ateitis*. doi:https://doi.org/10.3846/mla.2020.10562

Kankanhalli, A., Teo, H.-H. T., CY Tan, B., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International journal of information management 23, no. 2*, 139-154.

Kaplan, J. M., Bailey, T., O'Halloran, D., Marcus, A., & Rezek, C. (2015). *Beyond cybersecurity: protecting your digital business.* John Wiley & Sons.

Kianpour, M., Øverby, H. Ø., James Kowalski, S., & Frantz, C. (2019). Social preferences in decision making under cybersecurity risks and uncertainties. *International Conference on Human-Computer Interaction* (p. 149-163). Springer, Cham.

Knapp, K. J., E. Marshall, T., Rainer Jr, R. K., & W. Morrow., D. (2006). The top information security issues facing organizations: What can government do to help. *Network security 1*, 327.

Knowles, W., Prince, D., Hutchison, D., Ferdinand Pagna Disso, J., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection 9* , 52-80.

Kong, H.-K., Kim, T.-S. K., & Kim, J. (2012). An analysis on effects of information security investments: a BSC perspective. *Journal of Intelligent Manufacturing 23, no. 4*, 941-953.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & security 28, no. 7*, 509-520.

Krishnan, R., Martin, X., & G. Noorderhaven., N. (2006). When does trust matter to alliance performance? *Academy of Management journal 49, no. 5*, 894-917.

Kuklytė, J., & Ūsas, A. (2017). Informacinės visuomenės iššūkiai: kokios yra kibernetinių nusikaltimų formos? *Visuomenės saugumas ir viešoji tvarka*, 184-194.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security 105, 102248*.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management. *MIS Quarterly 31, no. 1*, 59–87. doi:https://doi.org/10.2307/25148781

Lietuvos Bankas. (2021 m. 10 22 d.). „FinTech“ plėtros skatinimui – palanki ir saugi aplinka. Nuskaityta iš https://www.lb.lt/lt/naujienos/fintech-pletros-skatinimui-palanki-ir-saugi-aplinka

Lietuvos Bankas. (2022). Finansų rinkos dalyvių priežiūra. Finansinės technologijos ir inovacijos. Nuskaityta iš https://www.lb.lt/lt/finansines-technologijos-ir-inovacijos

Lietuvos Respublikos seimas. (2018). Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas: 2018. m. birželio 27 d. Nr. XIII-1299. Vilnius. Nuskaityta iš https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/15e540727ac211e89188e16a6495e98c

Lietuvos statistikos departamentas. (2022 m. 10 12 d.). Kibernetinės atakos – rizika ne tik reputacijai. Nuskaityta iš https://osp.stat.gov.lt/straipsnis-kibernetines-atakos

LR rašto apsaugos Ministerija. (2022 m. 02 25 d.). Kibernetinis saugumas: NKSC įspėja dėl padidėjusios kibernetinio saugumo rizikos. Nuskaityta iš https://kam.lt/nksc-ispeja-del-padidejusios-kibernetinio-saugumo-rizikos/

Maharjan, R., & Chatterjee, J. M. (2019). Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal. *LBEF Research Journal of Science, Technology and Management, 1(1), 82-98*, 82-98.

Malčiauskaitė, D., & Kvietkauskienė, A. (2019). FinTech plėtros galimybės ir iššūkiai . *22-osios Lietuvos jaunųjų mokslininkų konferencijos „Mokslas – Lietuvos ateitis“ teminė konferencija.*

McKeen, J. D., & Smith, H. A. (2009). Developments in practice XXXIII: A holistic approach to managing IT-based risk. *Communications of the Association for Information Systems 25(1)*, 41.

Michael, H., & Champy, J. (2009). *Reengineering the Corporation: Manifesto for Business Revolution.* New York: NY: Harper Business.

Milena, V., & Radoica, L. (2022). Fintech, Risk-Based Thinking and Cyber Risk. *Journal of Central Banking Theory and Practice, 11(2)*, 27-53.

Moen, R., & Norman, C. (2009). Evolution of the PDCA Cycle.

Moşteanu, N. R. (2020). Challenges for Organizational Structure and design as a result of digitalization and cybersecurity. *The Business & Management Review 11.1* , 278-286.

Nacionalinis kibernetinio saugumo centras. (2022). Kibernetinio saugumo vadovas verslui. *Kibernetinis saugumas ir verslas - ką turėtų žinoti kiekvienas vadovas.*

Norvaišienė, R. (2005). *Įmonės investicijų valdymas.* Kaunas: KTU leidykla Technologija.

OECD. (2017). Enhancing the Role of Insurance in Cyber Risk Management. doi:http://dx.doi.org/10.1787/9789264282148-en

Panetta, F. (2018). Fintech and banking: today and tomorrow. *Annual Reunion of the Harvard Law School Association of Europe. Speech by the Deputy Governor of the Bank of Italy.*

ROCKIT VILNIUS. (2022). *Rockit Fintech Map 2022*. Nuskaityta iš https://www.rockitvilnius.com/database

Rolland, C. (1993). Modeling the Requirements Engineering Process. Nuskaityta iš https://www.researchgate.net/publication/2824908

Rolland, C. (1998). A Comprehensive View of Process Engineering. *International Conference on Advanced information Systems Engineering*, (p. 1-24). Nuskaityta iš https://hal.archives-ouvertes.fr/hal-00707940/document

Sackmann, S. (2008). A Reference Model for Process-Oriented IT Risk. *European Conference on Information Systems (ECIS)*, 246.

Savić, A. (2008). Managing IT-related operational risks. *Economic annals 53.176*, *53*(176), 88-109.

Seppänen, N. (2020). *Coopetition strategies of cybersecurity companies in Finnish markets.*

Setianingsih, L. S., Pulungan, R., Putra, A. E., Wibowo, M. E., & Syarip. (2021). Risk Assessment Methods for Cybersecurity in Nuclear Facilities: Compliance to Regulatory Requirements. *International Journal of Advanced Computer Science and Applications(IJACSA), 12(9),* 714-722. doi:http://dx.doi.org/10.14569/IJACSA.2021.0120979

Shaikha, H., Ali, M., Kurnia, S. K., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications, 58, 102726*.

Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A: Policy and Practice*, 523-536. doi:https://doi.org/10.1016/j.tra.2018.06.033

Shimonski, R. (2016). *CEH v9: Certified Ethical Hacker Version 9 Study Guide.* John Wiley & Sons.

Sianipar, C. P., Yudoko, G., & Dowaki, K. (2014). Physiological Concept: Visible Modeling for Feasible Design. *Applied Mechanics and Materials*, 493.

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of power: A study of mandated compliance to an information systems security" De Jure" standard in a government organization. *MIS quarterly (2010)*, 463-486.

Soomro, Z. A., Hussain Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management 36, no. 2*, 215-225.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication 800(30)*, 800-30.

201, R., & Černevičiūtė, J. (2014). Verslo procesų identifikavimas kūrybinių industrijų įmonių veiklos tobulinimo kontekste. *Tarptautinis verslas: inovacijos, psichologija, ekonomika (8)*, 14-26.

Strupczewski, G. (2021). Defining cyber risk. *Safety Science, 135*. doi:https://doi.org/10.1016/j.ssci.2020.105143

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management 17, no. 2*, 179-186.

Tsou, H.-T., & Hsuan-Yu Hsu, S. (2015). Tsou, Hung-Tai, and Sheila Hsuan-Yu Hsu. "Performance effects of technology–organization–environment openness, service co-production, and digital-resource readiness: The case of the IT industry. *International Journal of Information Management 35, no. 1*, 1-14.

Ulbinaitė, A., & Gribovskis, J. (2020). Žinių valdymo procesų ir verslo procesų integracijos sąveikos vertinimo modelis. *Informacijos mokslai, 88*, 142-166.

Umara, N., Anwar, Z., Amjad, T., & Raymond, K.-K. C. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems, 96,*, 227-242.

Valackienė, A. (2007). *Sociologinis tyrimas: vadovėlis.* Kaunas: KTU leidykla Technologija.

Wall, J., Benjamin Lowry, P., & B. Barlow, J. (2015). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems 1*, 39-76.

Westerman, G., & Hunter, R. (2007). IT risk: turning business threats into competitive advantage. 2-7.

Wilson, R. (2019). *20 Questions Directors Should Ask about Cybersecurity*. CISSP.

Wixom, B. H., & J. Watson, H. (2001). An empirical investigation of the factors affecting data warehousing success. *MIS quarterly*, 17-41.

Zhu, K., & L. Kraemer, K. (2005). Post-adoption variations in usage and value of e-business by organizations: cross-country evidence from the retail industry. *Information systems research 16, no. 1*, 61-84.

IMPACT OF CYBER RISK MANAGEMENT ON COMPANIES' PERFORMANCE RESULTS

Deimantė Jotautaitė

Master thesis

Strategic management of information systems master study programme

Vilnius University, Faculty of Economics and Business Administration

Supervisor - doc. dr. Mindaugas Krutinis

Vilnius, 2022

SUMMARY

87 pages, 14 tables, 15 pictures, 97 references

As companies become increasingly dependent on digital information, so do cyber risks. Cyber incidents could have a negative impact on the organization's performance. The main purpose of this master thesis is to determine the impact of cyber risk management on companies' performance results. The work consists of three main parts: the analysis of literature, the research methodology and research results analysis. Conclusions and recommendations based on research findings are presented at the end of the work.

Literature analysis includes cyber risk definition, the classification of cyber incidents, the concept of cyber security and its main components. Factors which affect cyber security readiness of organization are presented as well as the importance of cyber risk management for company financial and non-financial performance results. Literature analysis part is concluded with the clarification of the sectors most affected by cyber-attacks and description of Fintech sector in Lithuania.

After the literature analysis the author presents research methodology. Since the Fintech sector is one of the most affected by cyber-attacks, Fintech companies were selected as research units. The main purpose of the quantitative survey questionnaire was to define the factors which affect cyber security readiness of organization and to find out the influence of the cyber security on the performance results the Fintech sector companies in Lithuania. Representatives of Fintech companies operating in Lithuania were requested to rate research statements using Likert scale.

The results of the research were statistically processed with the SPSS program. In order to establish a correlation between cyber security factors and cyber security readiness of organization as well as between cyber security effectiveness and organization performance results Pearson's and Spearman's correlation coefficients were used. Furthermore, regression analysis to test the research hypotheses was applied.

The performed research revealed that direct relationship between all research constructs exists. Besides, organization culture and employees' skills are the main factors which impact the organizations capability to combat cyber-attacks attacks. Moreover, based on research results cyber security readiness significantly influences organizational cyber security performance which have the impact on financial and non-financial performance results in the Fintech companies operating in Lithuania.

The conclusions and recommendations summarize the main concepts of literature analysis as well as the results of the performed research. The author believes that the results of the study

could give useful advice to the companies how to strengthen cyber risk management factors that would contribute to the improvement of company security and its performance results.

Keywords: cyber risk, cyber risk management, cyber security, cyber security factors, companies‘ performance results, financial and non-financial performance results.

PRIEDAI

1 priedas. Pirminė tyrimo anketinė apklausa

IT Infrastruktūra	
1.	IT1: Turime pakankamai IT specialistų kibernetiniam saugumui valdyti.
2.	IT2: Turime IT infrastruktūrą, reikalingą kibernetiniam saugumui valdyti.
3.	IT3: Mes geriau išnaudojame IT išteklius kibernetinio saugumo srityje.
4.	IT4: Mes geriau panaudojame pažangias IT priemones ir metodus.
Aukščiausiosios vadovybės palaikymas	
5.	VP1: Aukščiausiajai vadovybei kibernetinis saugumas yra strategiškai svarbus.
6.	VP2: Aukščiausioji vadovybė demonstruoja įsipareigojimą kibernetiniam saugumui kuriant politiką/gaires.
7.	VP3:Aukščiausioji vadovybė prisiima atsakomybę už kibernetinį saugumą.
8.	VP4: Aukščiausioji vadovybė asmeniškai įsitraukia į susijusius klausimus
9.	VP5: Aukščiausia vadovybė remia kibernetinio saugumo iniciatyvas.
10.	VP6: Aukščiausioji vadovybė palaiko kibernetinio saugumo gerinimo procesus.
11.	VP7: Aukščiausioji vadovybė suformuluoja organizacijos tobulinimo viziją kibernetinis saugumas ateityje.
12.	VP8: Aukščiausioji vadovybė suformuluoja kibernetinių tinklų mažinimo strategiją
13.	VP9: Aukščiausioji vadovybė nustato tikslus ir standartus, kuriuos reikia stebėti ir sumažinti kibernetinio saugumo incidentus.
Darbuotojų įgūdžiai	
14.	OS1: Mūsų organizacijos darbuotojai turi reikiamų kibernetinio saugumo įgūdžių.
15.	OS2: Mūsų organizacija reguliariai moko personalą apie kibernetinio saugumo priemones ir metodus.
16.	OS3: Mūsų organizacija teikia išteklius personalo mokymui kibernetinio saugumo klausimais.
Organizacijos kultūra	
17.	OC1: mūsų organizacijoje dalijimąsi saugumo žiniomis įvairiuose organizacijos padaliniuose.
18.	OC2: Mūsų organizacijoje dalijimąsi informacija apie kibernetinio saugumo incidentus.
19.	OC3: Mūsų organizacijoje dalijimąsi informacija apie kibernetinio saugumo incidentų pasekmes.
20.	OC4: Mūsų organizacija skatina komandos narius prisidėti prie organizacijos kibernetinio saugumo gerinimo.
21.	OC5: Mūsų organizacija remia veiklos koordinavimą tarp skirtingų padalinių, kad pagerintų kibernetinį saugumą.
22.	OC6: Mūsų organizacijoje skatinamas bendradarbiavimas kibernetinio saugumo problemų sprendimui.
23.	OC7: Mūsų organizacijoje svarbu laikytis taisyklių ir išlaikyti saugiai veikiančią organizaciją.
24.	OC8: Mūsų organizacijoje yra įsipareigojimas plėtoti saugumo plėtrai.
Bendradarbiavimas su konkurentais	
25.	CC1: Dalijimasis informacija apie kibernetinius incidentus su konkurentais stiprina mūsų saugumą.

26.	CC2: Mūsų organizacija reguliariai bendrauja su konkurentais, kad pasidalintų informacija apie kibernetinius incidentus.
27.	CC3: Mūsų organizacija naudoja žinias apie incidentus, įgytas iš konkurentų patirties, siekdama greičiau išspręsti problemas.
28.	CC4: mūsų organizacija bendradarbiauja su konkurentais saugumo gerinimui.
29.	CC5: Mūsų organizacija naudoja naujas konkurentų idėjas ir įgūdžius, kad pagerintų savo saugumą.
30.	CC5: Mūsų organizacija naudoja naujas iš konkurentų patirties gautas idėjas ir įgūdžius, kad pagerintų savo saugumą.
Partnerių santykiai	
31.	SPR1: Mūsų organizacija mano, kad pažeidimo atveju mūsų tiekėjai / verslo partneriai elgsis mūsų interesais.
32.	SPR2: Jei mūsų organizacijai prireiktų pagalbos, mūsų verslo partneriai padarys viską, ką gali , kad padėtų
33.	SPR3: Mūsų verslo partneriai domisi ne tik savo, bet ir mūsų organizacijos gerove.
34.	SPR4: mūsų organizacija bendradarbiauja su verslo partneriais siekdama atsakomybės už saugumą.
35.	SPR5: Mūsų organizacija atvirai bendrauja su verslo partneriais.
Valstybės reguliavimas	
36.	GR1: valstybės taisyklės ir reglamentai yra svarbūs siekiant apsaugoti mūsų kibernetinę infrastruktūrą ir paslaugas, kad būtų imtasi atitinkamų atsakomųjų priemonių.
37.	GR2: Valstybė nustato verslo įstatymus, kad apsaugotų mūsų el. verslo sandorius.
38.	GR3: Valstybės reguliuoja internetą, kad jis taptų patikima verslo platforma (pvz., kovojant su sukčiavimu ir piktnaudžiavimu kredito kortelėmis).
Valstybės parama	
39.	GS1: Valstybės parama yra svarbi siekiant paskatinti mus gerinti savo saugumą.
40.	GS2: Valstybė kuria kibernetinio saugumo informavimo programas (pvz., kibernetinio saugumo seminarus)
41.	GS3: Valstybė dažnai informuoja mus apie naujausias kibernetines atakas, kad imtumėmės atitinkamų atsakomųjų priemonių.
Pramonės šakos standartai	
42.	IS1: standartų laikymasis padidina organizacijos kibernetinį saugumą.
43.	IS2: standartų laikymasis sumažina organizacijos kibernetinių incidentų skaičių
44.	IS3: standartų laikymasis sumažina organizacijos kibernetinių incidentų nesėkmių skaičių.
Kibernetinio saugumo pasirengimas	
45.	<u>Identifikavimas:</u> CSRI1 Mūsų organizacija žino ir yra įsipareigojusi naudoti pažangius pažeidžiamumo vertinimo metodus.
46.	CSRI2: Mūsų organizacija yra įsipareigojusi kontroliuoti kompiuterių prievadus, kurie gali būti naudojami atakoms.
47.	CSRI3: Mūsų organizacija yra įsipareigojusi užtikrinti, kad sistemos pažeidžiamumai būtų priimtinos rizikos ribose.
48.	<u>Apsauga:</u> CSRP1: mūsų organizacija žino ir yra įsipareigojusi naudoti duomenų šifravimą galutiniame taške.
49.	CSRP2: Mūsų organizacija žino ir yra įsipareigojusi naudoti apsaugos nuo virusų programinę

	įrangą.
50.	CSRP3: mūsų organizacija žino ir yra įsipareigojusi laikytis griežtos slaptažodžių politikos.
51.	Aptikimas: Mūsų organizacija žino ir yra įsipareigojusi įgalinti aktyvų kylančių grėsmių valdymą prieš joms atsirandant (pvz., grėsmių žvalgyba).
52.	CSRD2: Mūsų organizacija žino ir yra įsipareigojusi atlikti operatyvinę ir strateginę paskelbtų saugumo incidentų analizę
53.	CSRD3: mūsų organizacija žino ir yra įsipareigojusi nuolat stebėti saugos įspėjimus, kad nustatytų kibernetines atakas
54.	Atsakymas CSRR1: mūsų organizacija žino ir yra pasirengusi reaguoti į galimas atakas.
55.	CSRRs2: mūsų organizacija žino ir yra įsipareigojusi turėti sistemą, skirtą stebėti pertrūkį.
56.	CSRR3: mūsų organizacija žino ir įsipareigojo planuoti atsigavimą po kibernetinių atakų.
57.	Atkūrimo CSRRc1: mūsų organizacija žino ir įsipareigojo turėti atkūrimo plano įgyvendinimo procedūras.
58.	CSRRc2: Mūsų organizacija yra įsipareigojusi atsigauti po nesėkmės, saugodama ir atnaujindama atsargines duomenų bazes.
Organizacijos saugumo efektyvumas	
59.	OSP1: duomenų pažeidimų skaičius mūsų organizacijoje laikui bėgant mažėja.
60.	OSP2: mūsų organizacija turi teisėtą saugos reputaciją.
61.	OSP3: vidiniai mūsų organizacijos procesai tampa saugesni.
62.	OSP4: mūsų organizacijos duomenų bazės pasiekiamos, kai tik reikia.
63.	OSP5: Mūsų organizacija turi patikimą sistemą su tinkamomis informacijos apdorojimo galimybėmis ir pajėgumais.
Finansiniai rezultatai	
64.	Mūsų organizacija padidino pardavimus ir pelningumą per pastaruosius kelerius metus.
65.	FP2: mūsų organizacija per pastaruosius kelerius metus pasiekė pelno tikslus.
66.	FP3: mūsų organizacija per pastaruosius kelerius metus pasiekė pardavimo tikslus
67.	FP4: Mūsų organizacija per pastaruosius kelerius metus pasiekė rinkos dalies tikslus
Ne finansiniai rezultatai	
68.	NFP1: mūsų organizacija per pastaruosius kelerius metus pagerino esamų klientų lojalumą.
69.	NFP2: per pastaruosius kelerius metus mūsų organizacija pritraukė daug naujų klientų
70.	NFP3: mūsų organizacija pastaruosius kelerius metus turėjo svarbų konkurencinį pranašumą.
71.	NFP4: per pastaruosius kelerius metus mūsų organizacijos įvaizdis buvo gerai suvokiamas.
72.	NFP5: mūsų organizacija pastaruosius kelerius metus turėjo gerą reputaciją.

2 priedas. Galutinė tyrimo anketinė apklausa

Sveiki,

Esu Vilniaus Universiteto 2 kurso magistro studentė Deimantė Jotautaitė. Šiuo metu atlieku baigiamojo darbo tyrimą. Darbo tema - kibernetinės rizikos valdymo įtaka įmonių veiklos rezultatams.

Šiuo tyrimu siekiama išsiaiškinti kaip kibernetinio saugumo priemonės veikia įmonės veiklos finansinius ir ne finansinius rezultatus.

Pažymėkite teiginius skalėje: 1 = "visiškai nesutinku", 2 = "nesutinku", 3 = "neutralus", 4= „sutinku“, 5 = „visiškai sutinku“. Iš anksto dėkoju už atsakymus!

IT infrastruktūra (IT)	
1.	IT1: Turime pakankamai IT specialistų kibernetiniam saugumui valdyti.
2.	IT2: Turime IT infrastruktūrą, reikalingą kibernetiniam saugumui valdyti.
Organizacijos kultūra (OK)	
3.	OK1: Aukščiausioji vadovybė demonstruoja įsipareigojimą kibernetiniam saugumui kuriant politiką/gaires.
4.	OK2: Aukščiausia vadovybė remia kibernetinio saugumo iniciatyvas ir palaiko kibernetinio saugumo gerinimo procesus.
5.	OK3: Mūsų organizacija skatina darbuotojus prisidėti prie organizacijos kibernetinio saugumo gerinimo.
6.	OK4: Mūsų organizacijoje svarbu laikytis taisyklių ir išlaikyti saugiai veikiančią organizaciją.
Darbuotojų įgūdžiai (DI)	
7.	DI1: Mūsų organizacijos darbuotojai turi reikiamų kibernetinio saugumo įgūdžių.
8.	DI2: Mūsų organizacija moko darbuotojus ir teikia išteklius darbuotojų mokymui kibernetinio saugumo klausimais.
Bendradarbiavimas su konkurentais ir partneriais (BKP)	
9.	BKP1: Mūsų organizacija bendradarbiauja su konkurentais dėl saugumo gerinimo ir naudoja iš konkurentų įgytą patirtį, siekdama greičiau išspręsti problemas.
10.	PKP2: Mūsų organizacija atvirai bendrauja su verslo partneriais siekdama atskaitomybės už saugumą.
Valstybės reguliavimas ir parama, Pramonės šakos standartai	
11.	V1: Valstybės taisyklės ir reglamentai yra svarbūs siekiant apsaugoti mūsų kibernetinę infrastruktūrą ir paslaugas, kad būtų imtasi atitinkamų atsakomųjų priemonių.
12.	V1: Valstybės parama yra svarbi siekiant paskatinti mus gerinti savo saugumą.
13.	S1: Pramonės šakos standartų laikymasis stiprina organizacijos kibernetinį saugumą.

Kibernetinio saugumo pasirengimas	
14.	*Identifikavimas* KS1: Mūsų organizacija žino ir yra įsipareigojusi naudoti pažangius pažeidžiamumo vertinimo metodus.
15.	Apsauga: KS3: Mūsų organizacija žino ir yra įsipareigojusi naudoti duomenų šifravimą, apsaugos nuo virusų programinę įrangą ir laikytis griežtos slaptažodžių politikos.
16.	*Aptikimas ir reakcija:* KS5: Mūsų organizacija žino ir yra įsipareigojusi nuolat stebėti saugos įspėjimus, kad nustatytų kibernetines atakas ir yra pasirengusi į jas reaguoti.
17.	Atsistatymas: KS7: Mūsų organizacija žino ir įsipareigojus turėti atkūrimo plano įgyvendinimo procedūras.
Organizacijos saugumo efektyvumas	
18.	OS1: Duomenų pažeidimų skaičius mūsų organizacijoje laikui bėgant mažėja.
19.	OS2: Mūsų organizacija turi teisėtą saugos reputaciją.
20.	OS3: Vidiniai mūsų organizacijos procesai tampa saugesni.
Finansiniai rezultatai	
21.	FR: Mūsų organizacija padidino pardavimus ir pelningumą per pastaruosius kelerius metus.
22.	FR2: Mūsų organizacija per pastaruosius kelerius metus pasiekė pelno tikslus.
23.	FP3: Mūsų organizacija per pastaruosius kelerius metus pasiekė pardavimo tikslus.
Ne finansiniai rezultatai	
24.	NFR1: Mūsų organizacija per pastaruosius kelerius metus pagerino esamų klientų lojalumą ir pritraukė naujų klientų.
25.	NFR3: Mūsų organizacija pastaruosius kelerius metus turėjo svarbų konkurencinį pranašumą.
26.	NFR5: Mūsų organizacija pastaruosius kelerius metus turėjo gerą reputaciją.

3 priedas. Tyrimo rezultatų suvestinė

Apklausos teiginiai	Atsakymų dažnis						Statistiniai rodikliai			
	Visiškai nesutinku	Nesutinku	Neutralu	Sutinku	Visiškai sutinku	Iš viso	Vidurkis	Mediana	Moda	Std. nuokrypis
Turime pakankamai IT specialistų kibernetiniam saugumui valdyti	4	8	11	25	24	72	3,79	4	4	1,19
Turime IT infrastruktūrą, reikalingą kibernetiniam saugumui valdyti	2	5	8	28	29	72	4,07	4	5	1,03
Aukš. vadovybė demonstruoja įsipareigojimą kibernetiniam saugumui kuriant politiką/gaires	2	6	7	21	36	72	4,15	4,5	5	1,08
Aukš. vadovybė remia kibernetinio saugumo iniciatyvas ir palaiko kibernetinio saugumo gerinimo procesus	0	5	4	14	49	72	4,49	5	5	0,89
Mūsų organizacija skatina darbuotojus prisidėti prie organizacijos kibernetinio saugumo gerinimo	2	3	10	23	34	72	4,17	4	5	1,01
Mūsų organizacijoje svarbu laikytis taisyklių ir išlaikyti saugiai veikiančią organizaciją	1	1	5	18	47	72	4,51	5	5	0,81
Mūsų organizacijos darbuotojai turi reikiamų kibernetinio saugumo įgūdžių	1	6	18	35	12	72	3,71	4	4	0,9
Mūsų organizacija reguliariai moko darbuotojus apie kibernetinio saugumo priemones ir metodus	6	8	9	22	27	72	3,78	4	5	1,29
Mūsų organizacija bendradarbiauja su konkurentais dėl saugumo gerinimo ir naudoja iš konkurentų įgytą patirtį, siekdama greičiau išspręsti problemas	12	19	21	13	7	72	2,78	3	3	1,21
Mūsų organizacija atvirai bendrauja su verslo partneriais siekdama atskaitomybės už saugumą	4	4	15	22	27	72	3,89	4	5	1,15
Valstybės taisyklės ir reglamentai yra svarbūs siekiant apsaugoti mūsų kibernetinę infrastruktūrą ir paslaugas	4	6	14	24	24	72	3,81	4	4	1,16
Valstybės parama yra svarbi siekiant paskatinti mus gerinti mūsų saugumą	6	9	19	15	23	72	3,56	4	5	1,29
Pramonės šakos standartų (ISO,NIST) laikymasis stiprina organizacijos kibernetinį saugumą	1	6	12	22	31	72	4,06	4	5	1,03
Mūsų organizacija žino ir yra įsipareigojusi naudoti pažangius pažeidžiamumo vertinimo metodus	1	2	10	23	36	72	4,26	4,5	5	0,9

Mūsų organizacija žino ir yra įsipareigojusi naudoti duomenų šifravimą, apsaugos nuo virusų programinę įrangą ir laikytis griežtos slaptažodžių politikos	1	1	4	16	50	72	4,57	5	5	0,78
Mūsų organizacija žino ir yra įsipareigojusi nuolat stebėti saugos įspėjimus, kad nustatytų kibernetines atakas ir yra pasirengusi į jas reaguoti	2	2	4	16	48	72	4,47	5	5	0,93
Mūsų organizacija žino ir yra įsipareigojusi turėti atkūrimo plano įgyvendinimo procedūras	1	2	7	14	48	72	4,47	5	5	0,89
Duomenų pažeidimų skaičius mūsų organizacijoje laikui bėgant mažėja	1	4	25	16	26	72	3,86	4	5	1,03
Mūsų organizacija turi teisėtą saugos reputaciją	0	4	7	17	44	72	4,4	5	5	0,88
Vidiniai mūsų organizacijos procesai tampa saugesni	0	3	6	19	44	72	4,44	5	5	0,82
Mūsų organizacija padidino pardavimus ir pelningumą per pastaruosius kelerius metus	1	2	11	15	43	72	4,35	5	5	0,94
Mūsų organizacija per pastaruosius kelerius metus pasiekė pelno tikslus	3	6	14	21	28	72	3,9	4	5	1,14
Mūsų organizacija per pastaruosius kelerius metus pasiekė pardavimo tikslus	3	5	15	18	31	72	3,96	4	5	1,14
Mūsų organizacija per pastaruosius kelerius metus pagerino esamų klientų lojalumą ir pritraukė naujų klientų	2	2	9	23	36	72	4,24	4,5	5	0,97
Mūsų organizacija per pastaruosius kelerius metus turėjo svarbų konkurencinį pranašumą	1	8	10	32	21	72	3,89	4	4	1
Mūsų organizacija pastaruosius kelerius metus turėjo gerą reputacija	2	0	4	22	44	72	4,47	5	5	0,84

Correlations

			IT	OK	DI	BKP	VRPS	KS	S	FR	NFR
Spearman's rho	IT	Correlation Coefficient	1,000	,669**	,482**	,382**	,365**	,365**	,334**	,161	,207
		Sig. (2-tailed)	.	<,001	<,001	<,001	,002	,002	,004	,176	,081
		N	72	72	72	72	72	72	72	72	72
	OK	Correlation Coefficient	,669**	1,000	,699**	,595**	,350**	,646**	,576**	,261*	,464**
		Sig. (2-tailed)	<,001	.	<,001	<,001	,003	<,001	<,001	,027	<,001
		N	72	72	72	72	72	72	72	72	72
	DI	Correlation Coefficient	,482**	,699**	1,000	,609**	,269*	,574**	,517**	,231	,379**
		Sig. (2-tailed)	<,001	<,001	.	<,001	,022	<,001	<,001	,051	,001
		N	72	72	72	72	72	72	72	72	72
	BKP	Correlation Coefficient	,382**	,595**	,609**	1,000	,060	,512**	,454**	,235*	,217
		Sig. (2-tailed)	<,001	<,001	<,001	.	,617	<,001	<,001	,047	,067
		N	72	72	72	72	72	72	72	72	72
	VRPS	Correlation Coefficient	,365**	,350**	,269*	,060	1,000	,195	,495**	,325**	,436**
		Sig. (2-tailed)	,002	,003	,022	,617	.	,101	<,001	,005	<,001
		N	72	72	72	72	72	72	72	72	72
	KS	Correlation Coefficient	,365**	,646**	,574**	,512**	,195	1,000	,633**	,323**	,413**
		Sig. (2-tailed)	,002	<,001	<,001	<,001	,101	.	<,001	,006	<,001
		N	72	72	72	72	72	72	72	72	72
	S	Correlation Coefficient	,334**	,576**	,517**	,454**	,495**	,633**	1,000	,392**	,539**
		Sig. (2-tailed)	,004	<,001	<,001	<,001	<,001	<,001	.	<,001	<,001
		N	72	72	72	72	72	72	72	72	72
	FR	Correlation Coefficient	,161	,261*	,231	,235*	,325**	,323**	,392**	1,000	,630**
		Sig. (2-tailed)	,176	,027	,051	,047	,005	,006	<,001	.	<,001
		N	72	72	72	72	72	72	72	72	72
	NFR	Correlation Coefficient	,207	,464**	,379**	,217	,436**	,413**	,539**	,630**	1,000
		Sig. (2-tailed)	,081	<,001	,001	,067	<,001	<,001	<,001	<,001	.
		N	72	72	72	72	72	72	72	72	72

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Correlations

		IT	OK	DI	BKP	VRPS	KS	S	FR	NFR
IT	Pearson Correlation	1	,690**	,552**	,385**	,423**	,540**	,453**	,212	,304**
	Sig. (2-tailed)		<,001	<,001	<,001	<,001	<,001	<,001	,074	,010
	N	72	72	72	72	72	72	72	72	72
OK	Pearson Correlation	,690**	1	,717**	,600**	,476**	,713**	,712**	,382**	,540**
	Sig. (2-tailed)	<,001		<,001	<,001	<,001	<,001	<,001	<,001	<,001
	N	72	72	72	72	72	72	72	72	72
DI	Pearson Correlation	,552**	,717**	1	,612**	,281*	,645**	,636**	,367**	,469**
	Sig. (2-tailed)	<,001	<,001		<,001	,017	<,001	<,001	,002	<,001
	N	72	72	72	72	72	72	72	72	72
BKP	Pearson Correlation	,385**	,600**	,612**	1	,139	,449**	,458**	,282*	,233*
	Sig. (2-tailed)	<,001	<,001	<,001		,243	<,001	<,001	,016	,049
	N	72	72	72	72	72	72	72	72	72
VRPS	Pearson Correlation	,423**	,476**	,281*	,139	1	,273*	,503**	,354**	,526**
	Sig. (2-tailed)	<,001	<,001	,017	,243		,020	<,001	,002	<,001
	N	72	72	72	72	72	72	72	72	72
KS	Pearson Correlation	,540**	,713**	,645**	,449**	,273*	1	,754**	,353**	,508**
	Sig. (2-tailed)	<,001	<,001	<,001	<,001	,020		<,001	,002	<,001
	N	72	72	72	72	72	72	72	72	72
S	Pearson Correlation	,453**	,712**	,636**	,458**	,503**	,754**	1	,447**	,589**
	Sig. (2-tailed)	<,001	<,001	<,001	<,001	<,001	<,001		<,001	<,001
	N	72	72	72	72	72	72	72	72	72
FR	Pearson Correlation	,212	,382**	,367**	,282*	,354**	,353**	,447**	1	,739**
	Sig. (2-tailed)	,074	<,001	,002	,016	,002	,002	<,001		<,001
	N	72	72	72	72	72	72	72	72	72
NFR	Pearson Correlation	,304**	,540**	,469**	,233*	,526**	,508**	,589**	,739**	1
	Sig. (2-tailed)	,010	<,001	<,001	,049	<,001	<,001	<,001	<,001	
	N	72	72	72	72	72	72	72	72	72

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,744[a]	,553	,519	,53890

a. Predictors: (Constant), VRPS, BKP, IT, DI, OK

b. Dependent Variable: KS

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	23,736	5	4,747	16,347	<,001[b]
	Residual	19,167	66	,290		
	Total	42,903	71			

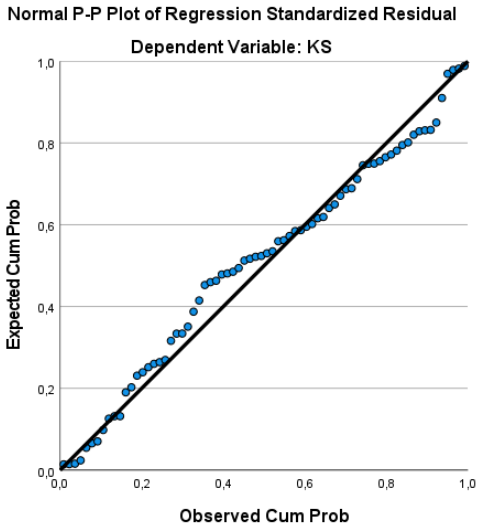
a. Dependent Variable: KS

b. Predictors: (Constant), VRPS, BKP, IT, DI, OK

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	1,600	,371		4,313	<,001		
	IT	,056	,089	,073	,626	,534	,501	1,995
	OK	,518	,146	,539	3,544	<,001	,293	3,418
	DI	,221	,099	,281	2,225	,029	,425	2,351
	BKP	-,049	,087	-,063	-,565	,574	,550	1,818
	VRPS	-,073	,084	-,085	-,874	,385	,723	1,383

a. Dependent Variable: KS



Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,754[a]	,568	,562	,51913

a. Predictors: (Constant), KS

b. Dependent Variable: S

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	24,788	1	24,788	91,981	<,001[b]
	Residual	18,865	70	,269		
	Total	43,653	71			

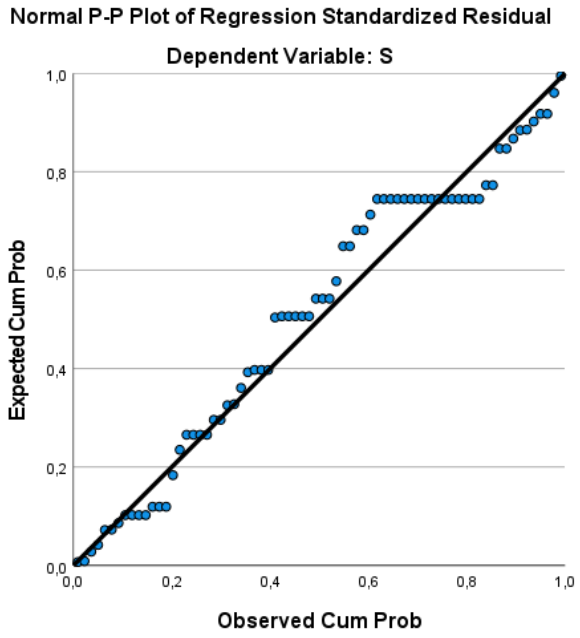
a. Dependent Variable: S

b. Predictors: (Constant), KS

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	,858	,358		2,399	,019		
	KS	,760	,079	,754	9,591	<,001	1,000	1,000

a. Dependent Variable: S



Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,447[a]	,200	,188	,88316

a. Predictors: (Constant), S

b. Dependent Variable: FR

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	13,611	1	13,611	17,450	<,001[b]
	Residual	54,598	70	,780		
	Total	68,208	71			

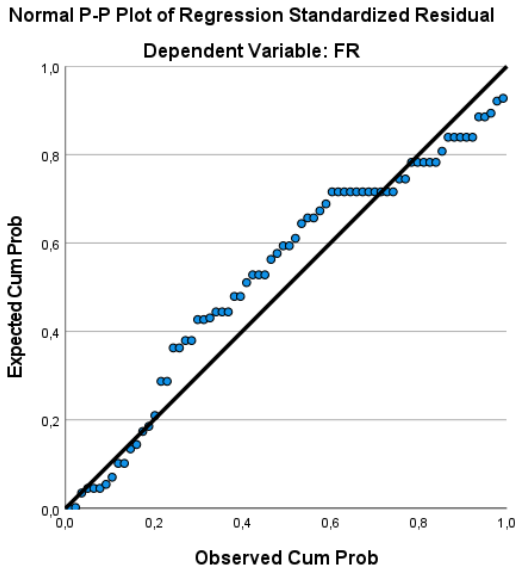
a. Dependent Variable: FR

b. Predictors: (Constant), S

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	1,704	,576		2,960	,004		
	S	,558	,134	,447	4,177	<,001	1,000	1,000

a. Dependent Variable: FR



Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,589[a]	,347	,338	,65429

a. Predictors: (Constant), S

b. Dependent Variable: NFR

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	15,958	1	15,958	37,278	<,001[b]
	Residual	29,966	70	,428		
	Total	45,924	71			

a. Dependent Variable: NFR

b. Predictors: (Constant), S

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	1,638	,427		3,840	<,001		
	S	,605	,099	,589	6,106	<,001	1,000	1,000

a. Dependent Variable: NFR