VILNIUS TECH
Vilnius Gediminas Technical University

24-osios Lietuvos jaunųjų mokslininkų konferencijos „Mokslas – Lietuvos ateitis“ teminė konferencija
Proceedings of the 24th Conference for Junior Researchers “Science – Future of Lithuania”

EKONOMIKA IR VADYBA / ECONOMICS AND MANAGEMENT

eISSN 2029-7149
2021 m. spalio 21 d., Vilnius, Lietuva
21 October 2021, Vilnius Lithuania
eISBN 978-609-476-279-6
Article Number: vvf.2021.051

Finansų valdymas / Financial Management
http://jmk.vvf.vilniustech.lt

INFORMACINIŲ TECHNOLOGIJŲ ĮMONĖS RIZIKŲ VERTINIMAS DIEGIANT FINANSINES TECHNOLOGIJAS

Augustina DUMPYTĖ*, Indrė LAPINSKAITĖ

Vilniaus Gedimino technikos universitetas, Verslo vadybos fakultetas,
Finansų inžinerijos katedra, Saulėtekio al. 11, LT-10221, Vilnius, Lietuva
**El. paštas augustina.dumpyte@stud.vilniustech.lt*

Santrauka. Šiais laikais dėmesys finansinėms technologijoms (*Fintech*) ir jų procesams didėja. *Fintech* yra pripažintos vienomis iš svarbiausių finansų pramonės naujovių, kurios itin sparčiai vystosi, tad vis daugiau siekiama taikyti finansines technologijas ne tik finansų sektoriuje, bet ir informacinių technologijų (IT) įmonėse. Straipsnyje atskleidžiama *Fintech* sampratos esmė, turinys, formuluojamos pagrindinės *Fintech* inovacijų rūšys. Taip pat analizuojamos rizikos, su kuriomis gali susidurti IT įmonės, nusprendusios įmonės viduje įsidiegti *Fintech*, siekdamos automatizuoti įmonės procesus. Pagrindinis šio tyrimo tikslas yra išnagrinėti *Fintech* proceso diegimo galimas rizikas, atlikti jų vertinimą IT įmonėse. Tikslui pasiekti naudojama mokslinės literatūros šaltinių analizė ir sisteminimas, ekspertų apklausa, kiekybinis, kokybinis vertinimas, SSGG analizė, rizikų žemėlapis. Šiame straipsnyje atskleidžiamos didžiausios rizikos, kurios gali kilti IT įmonėje diegant *Fintech*.

Reikšminiai žodžiai: finansinės technologijos, rizika ir vertinimas, informacinės technologijos.

Įvadas

Šiuolaikinėje nuolat tobulėjančioje bei besikeičiančioje rinkoje įmonei, siekiančiai išlikti konkurencingai bei neatsiliekančiai nuo kitų verslų, privalu domėtis bei diegti versle naujausias technologijas (Ancri, 2016; Dadelytė & Mačiulytė-Šniukienė, 2019). Mokslininkai vieningai sutaria, kad būtent finansinės technologijos (*Fintech*) yra pripažintos viena iš svarbiausių pramonės naujovių, kuri itin sparčiai vystosi, pvz., mobilieji mokėjimai, biudžeto planavimo programėlės (Dhar & Stein, 2017; Edirisinghe Vincent & Pinsker, 2020; Gomber et al., 2018; Lee & Shin, 2018, Varga, 2017). Lietuva ir toliau sparčiai stiprina *Fintech* industriją, neužleisdama pirmaujančių pozicijų (Lietuvos Respublikos finansų ministerija, 2020). Visa tai įrodo, kad verslininkams privalu pagalvoti apie savo kuriamus produktus, turimus procesus bei galimybę juos atnaujinti pritaikant *Fintech*.

Dauguma mokslinės literatūros autorių (Gomber et al., 2018, Lee, & Shin, 2018) daugiausia analizuoja tik *Fintech* visuomenei sukeliamus teigiamus padarinius. Priešingai nei minėti autoriai, O. Kovacsas (Kovacs, 2018) savo moksliniuose straipsniuose teigia, kad *Fintech* industrija, bediegianti inovacijas, taip pat susiduria ir su neigiamomis pasekmėmis, kurios vėliau gali įmonei užtraukti baudas, licencijos atėmimą ar privesti įmonę prie bankroto. Su (Kovocs, 2018) nuomone sutinka ir kiti mokslininkai bei ekonomistai (Schwab, 2016; Schattenberg et al., 2018). Šie autoriai savo moksliniuose straipsniuose pritaria idėjai, kad *Fintech* revoliucija gali sukelti didesnę nelygybę, ypač dėl jos galimybių sutrikdyti darbo rinkas.

Pastaraisiais metais ypač matoma, kad finansinių bei informacinių technologijų (toliau – IT) taikymas bei naudojimas šiuolaikiniame gyvenime bei rizikų įvertinimo nebuvimas suformavo nesankcionuotos prieigos ir duomenų praradimo tikimybę (Edirisinghe Vincent & Pinsker, 2020; Vitkus et al., 2020). Kuo aukštesnis socialinių procesų informatizavimo lygis, tuo didesnė rizika ir platesnis kibernetinės saugos grėsmių spektras (Jevsejev, 2020). Pagal vieną didžiausių verslo teisės advokatų kontorą *Baker McKenzie* operacinė rizika verčia įmones pagalvoti apie rizikų valdymą (Baker McKenzie, 2020). Taigi, bendrovei, nusprendusiai naudotis *Fintech*, prieš pradedant vykdyti pakeitimus, būtina įsivertinti galimas rizikas.

Tyrimo problema – kokias *Fintech* rizikas reikia vertinti, siekiant įsidiegti Fintech IT įmonėse.

Tyrimo objektas: IT įmonės rizika.

Tyrimo tikslas: teoriškai pagrįsti ir įvertinti *Fintech* proceso diegimo rizikas, atlikti jų vertininimą IT įmonėje.

Tyrimo metodai: mokslinės literatūros šaltinių analizė ir sisteminimas, ekspertų apklausa, ekspertinis vertinimas, daugiakriteris vertinimas, kiekybinis, kokybinis vertinimas, SSGG analizė, rizikų žemėlapis.

1. Teorinė *Fintech*, IT bei rizikos literatūros analizė

1.1. *Fintech* ir IT samprata

Įmonei siekiant išlikti konkurencingai bei neatsiliekančiai nuo kitų verslų privalu domėtis bei diegti savo verslui naujausias technologijas (Ancri, 2016). Būtent *Fintech* yra pripažinta viena iš svarbiausių finansų pramonės naujovių, kuri itin sparčiai vystosi (Dhar & Stein, 2017; Gomber et al., 2018; Lee & Shin, 2018). *Fintech* yra pavyzdys, kuris puikiai apibūdina XXI amžiaus finansinių paslaugų sektorių. Šiais laikais šis terminas apima visas technologines naujoves finansų sektoriuje, įskaitant finansinio raštingumo, švietimo naujoves, investicijas, bankininkystę ir kita (Gomber et al., 2018). Spartų *Fintech* vystymąsi iš dalies lemia palankus reguliavimas, dalijimosi ekonomika bei svarbiausia – nuolat tobulėjančios IT (Lee & Shin, 2018).

Be visa to, literatūros šaltiniuose nurodoma, kad *Fintech* nebūtinai apsiriboja tik finansinėmis paslaugomis, kaip kad finansavimu, naujų verslo modelių kūrimu (pvz., P2P skolinimu). Šioje dalyje svarbu suprasti, kad *Fintech* kartu vykdo verslo operacijas, teikia paslaugas ir tiekia produktus kaip alternatyvą tradicinėms finansų įstaigoms (Arner et al., 2015). Apskritai *Fintech* yra novatoriškas šiuolaikinių nefinansinių institucijų produktas bei paslauga (Sweeney, 2017). Anot Thakor (Thakor, 2020), *Fintech* terminas apibrėžtas gana siauru požiūriu – *Fintech* yra technologijos, kurios naudojamos teikiant naujas ir patobulintas finansines paslaugas. Su tuo nesutiktų Chen, Wu ir Yang (2019) – jie teigia, kad nors finansinėmis technologijomis / inovacijomis galima plačiai apibrėžti bet kokią technologiją, kuri įgalina ar pagerina finansinių paslaugų teikimą, toks apibrėžimas yra neribotas.

Finansinės naujovės, ypač informacinių ir ryšių technologijų taikymas, lėmė perversmą finansų industrijoje ir darys tai ateityje. Bendras inovacijų apibrėžimas paaiškina, kad jos atsiranda, kai įgyvendinamos naujos idėjos, sprendimai ir priemonės, kad būtų galima pakeisti verslo subjekto sąlygas ir pagerinti jo padėtį. Finansinių inovacijų sąvoka gali būti apibrėžta kaip naujų finansinių produktų ir paslaugų kūrimas ir skatinimas, naujų procesų kūrimas siekiant palengvinti finansinę veiklą, bendrauti su klientais ir sukurti naujas finansų įstaigų struktūras (Manta, 2018). *Fintech* taip pat nurodo naujų IT, įskaitant didžiųjų duomenų, debesų kompiuterijos ir mobiliųjų technologijų, naudojimą siekiant pagerinti paslaugų kokybę ir valdymo efektyvumą bei išplėsti finansinių paslaugų sritį (Hu et al., 2019). Tad *Fintech* gali būti naudojamos ne tik finansinių įmonių, tačiau gali būti diegiamos ir novatoriškose IT įmonėse, siekiančiose gerinti savo produktus (Ryu, 2018).

Siekiant identifikuoti ir klasifikuoti realius *Fintech* pavyzdžius, iš kurių ateityje gali kilti rizika, prieš tai būtina nustatyti *Fintech* rūšis. Taigi, šiam tikslui įgyvendinti privalu išskirti atskiras *Fintech* kategorijas jas suskirstant pagal kategorijos / rūšies apibrėžimą, pagrindines šiai rūšiai naudojamas technologijas.

1 lentelė. *Fintech* samprata bei technologijos

Apibrėžimas	Pagrindinės technologijos
Kibernetinis saugumas: techninė arba programinė įranga, naudojama finansiniam privatumui užtikrinti bei apsaugoti nuo elektroninės vagystės ar sukčiavimo.	Biometrinis autentifikavimas, duomenų šifravimas, ženklinimas.
Mobiliosios operacijos: technologijos, palengvinančios mokėjimus mobiliaisiais belaidžiais įrenginiais.	Išmaniųjų telefonų, laikrodžių – apyrankių piniginės, kitos skaitmeninės piniginės.
Elektroninės operacijos: technologijos, palengvinančios mokėjimus naudojantis elektroniniais įrenginiais.	Elektroniai mokėjimai, atsiskaitymai kredito / debeto kortelėmis.
Duomenų analizė: technologijos ir algoritmai, palengvinantys sandorių duomenų ar vartotojų finansinių duomenų analizę.	Didieji duomenys (angl. – *Big data*), debesų kompiuterija (angl. – *Cloud computing*), dirbtinis intelektas, mašinų mokymasis (angl. – *Machine learning*).
„Blockchain“: priskirtos, naudojamos technologijos, kurios pirmiausia pritaikomos finansinėms paslaugoms.	Kriptovaliuta, darbo įrodymas (angl. – *Proof of work*), išmaniosios sutartys.

1 lentelės pabaiga

Apibrėžimas	Pagrindinės technologijos
Tarpusavio skolinimasis (angl. – *Peer to peer*): programinė įranga, sistemos ar platformos, kurios palengvina klientų mokėjimų operacijų atlikimą.	Sutelktinis finansavimas, tarpusavio skolinimas, kliento mokėjimai.
„Robotizuoti patarimai“ (angl. – *Robo-advising*): kompiuterinės sistemos ar programos, teikiančios automatizuotas investavimo konsultacijas klientams ar portfelio valdytojams.	Didieji duomenys (angl. – *Big data*), debesų kompiuterija (angl. – *Cloud computing*), dirbtinis intelektas, mašinų mokymasis (angl. – *Machine learning*), elektroninė prekyba.

Taigi, iš 1 lentelės matoma, kad *Fintech* galima išskaidyti net į septynias kategorijas, t. y. kibernetinį saugumą, mobiliąsias operacijas, duomenų analizę, „Blockchain“, tarpusavio skolinimąsi, „Robotizuotus patarimus“ bei elektronines operacijas. Taip pat iš 1 lentelės galima daryti išvadą, kad *Fintech* inovacijų rūšys gali būti gana plačios ir naudojamos ne tik *Fintech* įmonėse (pvz., dirbtinio intelekto ar duomenų analizės taikymas) arba, priešingai, inovacijos gali būti siauros ir taikomos tik *Fintech* įmonėse (pvz., tarpusavio skolinimasis ar „Blockchain“ technologijos).

Galiausiai, iš anksčiau pateiktos informacijos preziumuojama, kad ne visas inovacijas / IT galima priskirti *Fintech* inovacijoms, tačiau šiuolaikiniame pasaulyje inovacijos yra didelė *Fintech* dalis.

1.2. *Fintech* rizikos samprata, rūšys

Rizika ir rizikos valdymas yra neatskiriami dalykai kalbant apie verslą, jo vykdymą bei tobulėjimą. Siekiant geriau suprasti patį verslą, kaip jį valdyti, kaip didinti savo pajamas, būtina įvertinti tam tikras tam verslui būdingas rizikas, kurios gali turėti didelę reikšmę ateityje. Šiame straipsnyje pabrėžiama, kad rizika turi ne vieną apibrėžimą, kurios turinys naudojamas skirtingose srityse ir yra skirtingas (Stasytytė ir Aleksienė, 2015). Svarbiausiuose žodynuose ir knygose rizikos sąvoka apibūdinama kaip „1) ryžimasis veikti žinant, kad yra tam tikra tikimybė nepasiekti tikslo, arba ryžimasis nepaisyti galimų neigiamų atsitiktinių aplinkybių padarinių; 2) aplinkybės, kuriomis gali ištikti nesėkmė apsisprendusį imtis tam tikro veiksmo, priemonės ar jų nesiimti; 3) nepasisekimo tikimybė“ (Rutkauskas ir Stasytytė, 2011).

Praeitame skyriuje išsiaiškinta, kad rizika turi skirtingus apibrėžimus. Informacinės sistemos kontekste suvokiama rizika daro neigiamą įtaką IT ar informacinių sistemų paslaugų pritaikymui (Ryu, 2018). Nors finansų technologijos siūlo vis daugiau prieinamesnių sprendimų, kurie atitiktų skirtingo dydžio įmonių poreikius (Chanias et al., 2019), vienas iš svarbesnių punktų, kuriuos įmonei reikia įsivertinti – veiksniai, kurie gali būti svarbūs ir reikalingi diegiant šias technologijas. Anot autorių (Hynes, 2018; Moghni et al., 2020), diegiant *Fintech* svarbu atsižvelgti į vartotojų norus ir lūkesčius. Ryu (2018) nurodo, kad rizikos suvokimas yra gyvybiškai svarbus veiksnys, kai vartotojai svarsto apie *Fintech* naudojimą. Taigi, rizika gali būti apibrėžiama kaip „vartotojų įspūdis apie pažeidžiamumą ir galimas neigiamas su *Fintech* susijusias pasekmes“. Todėl ir IT įmonėms, prieš diegiant *Fintech* įmonės viduje, gerinant savo siūlomus produktus, būtina įsivertinti, ar toks jų sprendimas duos joms norimus rezultatus.

Riziką gali sukelti išoriniai ir vidiniai veiksniai, tad bendrai rizikos veiksnius galima klasifikuoti į dvi grupes (ISO 31000:2009, 2009): išoriniai rizikos veiksniai – įvykiai ir aplinkybės, staiga bei netikėtai veikiančios įmonę iš išorės, kurių negalima prognozuoti, užkirsti jiems kelio ar daryti esminės įtakos. Išorinė rizika dar skirstoma į tiesioginio poveikio veiksnius (tai įstatymai, mokesčių sistema, partnerių elgesys, korupcija ir reketas ir kt.) bei netiesioginio poveikio veiksnius (tai politinė ir ekonominė šalies situacija, rinkos dinamika, tarptautiniai įvykiai, stichinės nelaimės ir kt.). Vidiniai veiksniai – tai rizikos, užprogramuotos pačios įmonės veikloje. Pagrindiniai vidiniai rizikos veiksniai galėtų būti personalo rizika (personalo kaita, kvalifikacija ir kt.), informacijos ir proceso rizika (IT trukdžiai, nepakankama informacijos sklaida ir kt.), verslo partnerių rizika (priklausomybė nuo pagrindinių tiekėjų ir užsakovų), (Stasytytė ir Aleksienė, 2015). Moksliniuose šaltiniuose gilinantis į šių laikų informacines bei *Fintech* technologijas minimos keturios pagrindinės finansinės rizikos: kredito (tikimybė, kad tam tikri finansų sistemos segmentai gali patirti reikšmingų nuostolių dėl skolininkų įsipareigojimų nevykdymo), likvidumo (rizika, kad kita sandorio šalis už visą įsipareigojimo sumą atsiskaitys ne suėjus atsiskaitymo terminui, bet kada nors vėliau neapibrėžtu metu), rinkos (nuostolių, kuriuos gali patirti rinkos dalyviai dėl nepalankios dinamikos finansų rinkose, dydis) bei operacinė rizika (tikimybė patirti nuostolių dėl žmonių, sistemų, netinkamų ar nepavykusių vidaus procesų arba dėl išorės įvykių įtakos, įskaitant teisinę riziką)

(Heidary Dahooie et al., 2021; Tabasi et al., 2019). Šioje vietoje taip pat svarbu išskirti, kad IT sektoriui taikomi griežti informacijos saugumo reikalavimai, nes šiais laikais bendrovė, netinkamai įsidiegusi procesus, gali patirti IT vagystę, kitus kompiuterinius nusikaltimus (Janeliūnienė ir Davidavičienė, 2013).

2. Rizikos valdymo metodikos analizė

Rizikos valdymo metodikos analizė. Rizikai identifikuoti surandama ne viena metodologija ir / ar priemonė. Pavyzdžiui, 2004 m. Niujorke Committee of Sponsoring Organizations of the Treadway Commission [COSO] (2004) išleido „Organizacijos rizikų valdymo – integruotos sistemos (angl. *Enterprise Risk Managment – Integrated Framework*) metodologiją“ (toliau – COSO ERM). Pagrindinis COSO ERM standarto tikslas – padėti įmonės vadovams geriau susitvarkyti su rizika siekiant organizacijos tikslų. COSO ERM akcentuojamas lankstus rizikos vertinimo modelis, pagal kurį vertinamas visas bendras įmonės rizikos valdymo procesas, o ne sutelkiamas dėmesys į konkrečias veiklos rizikos valdymo proceso dalis (Stasytytė ir Aleksienė, 2015). 2009 m. buvo paskelbtas ISO 31000 rizikos valdymo standartas – principai ir įgyvendinimo gairės. ISO 31000 standarte pateikiamos rekomendacijos, kaip įgyvendinti rizikos valdymo procesą, suformuojami bet kokios formos rizikos sisteminio, skaidraus ir patikimo valdymo principai ir gairės bet kokia apimtimi ir bet kokiame kontekste. Šis skirtumas yra esminis, lyginant šias dvi populiariausias sistemas, leidžiantis suprasti, kaip modeliai gali būti naudojami. Įmonė, kuri siekia susidaryti rizikos valdymo planą, turėtų remtis pripažintais rizikos valdymo standartais, kurie nusako rizikos valdymo procesą.

Identifikuoti riziką padeda ir rizikų registro sudarymas. Rizikų registras yra dokumentas, kuriame registruojami visi iš anksto identifikuoti ir projekto valdymo metu įvykę rizikos įvykiai ir jų valdymo priemonės. Sąraše identifikuojamos rizikos kartu jas susiejant su įvykiais, kurie gali turėti įtakos įmonei, siekiančiai įvykdyti savo tikslus (šiuo atveju – siekiančiai įsidiegti *Fintech*). Taigi, svarbu nustatyti ne tik pačią riziką, bet ir jos šaltinį (įvykį ar sąlygą, kuri gali lemti rizikos pasireikškimą) bei rizikos pasekmes ar būsimą efektą (1 pav.), (2018).

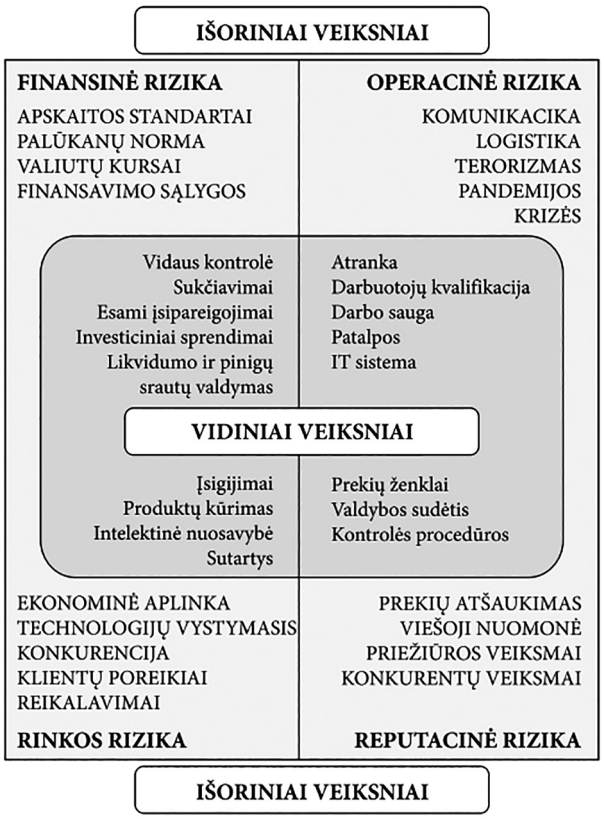
1 paveikslas. Rizikos, jos priežasčių ir pasekmių identifikavimas (sudaryta autorės)

Siekiant sudaryti rizikos registrų sąrašą / registrą, galima pasitelkti tokius rizikos identifikavimo metodus kaip minčių lietus (angl. *Branstorming*). Šis metodas taikomas žmonių grupėje, kurioje, pavyzdžiui, darbuotojai dalinasi savo idėjomis su kitais, kartu sukurdami naujas idėjas. Siekiant geriau identifikuoti rizikas, galima taikyti *Delfi* metodą, kurio metu infomacija apie rizikingus įvykius gaunama iš ekspertų. Taip pat galima tiesiog atlikti anketines ar žodines ekspertų apklausas (Janeliūnienė ir Davidavičienė, 2013; Martinkutė-Kaulienė ir Stasytytė, 2018).

SSGG analizės metodas. SSGG yra populiarus įrankis, padedantis vertinti galimas rizikas, jį taikant analizuojamos vidinė ir išorinė aplinkos, kuriose rizikos gali kilti (Kahraman et al., 2018). Bet kokios SSGG analizės tikslas yra nustatyti pagrindines organizacijos stiprybes ir silpnybes bei galimybes ir grėsmes aplinkoje. Stiprybės ir silpnybės grindžiamos organizacijos „vidaus auditu“. Galimybės ir grėsmės yra susijusios su „aplinkos veiksniais“, į kuriuos sprendimus priimantys asmenys turėtų atsižvelgti planuodami strateginius veiksmus. Galimybės yra aplinkos veiksniai, kuriuos galima naudingai išnaudoti, o į grėsmes reikia atsižvelgti, nes jos gali pakenkti organizacijai (Martinkutė-Kaulienė ir Stasytytė, 2018).

Strategijos kuriamos atsižvelgiant į esamas stiprybes, silpnybių pašalinimą, galimybių išnaudojimą ir grėsmių mažinimą. Taikant SSGG nustatomos stiprybės ir silpnybės atliekant vidinį įmonės vertinimą ir išorinį aplinkos vertinimą. Atliekant vidinį vertinimą nagrinėjami visi organizacijos aspektai, pvz., personalas, įrenginiai, vieta, produktai ir paslaugos, siekiant nustatyti organizacijos stiprybes ir silpnybes. Atliekant išorinį vertinimą tiriama politinė, ekonominė, socialinė, technologinė ir konkurencinė aplinka, siekiant nustatyti galimybes ir grėsmes (Lee, 2013). SSGG matricoje pateikiamos keturios strategijos alternatyvos, pagrįstos išorinių galimybių ir grėsmių suderinimu su organizaciniu požiūriu pagrįstomis vidinėmis stiprybėmis ir silpnybėmis (2 pav.).

Todėl šiame tyrime siekiant suprasti įmonės stiprybes, silpnybes, galimybes ir grėsmes bus atliekama SSGG analizė, vėliau sudaroma SSGG matrica, kuri padės įmonei suprasti, kaip galima išnaudoti stiprybes mažinant grėsmes, kaip pasinaudoti galimybėmis siekiant sumažinti silpnybes.



2 paveikslas. Rizikos veiksnių pavyzdžiai (AIRMIC, ALARM, IRM, 2010)

Ekspertinio vertinimo metodas. Tai procedūra, leidžianti suderinti atskirų ekspertų nuomones ir suformuoti bendrą sprendimą (Serikovienė, 2013). Pasak mokslininkų (Tidikis, 2003), šis metodas yra tinkamiausias duomenims patikrinti arba pagrįsti. Tam pritaria ir kiti mokslininkai (Burkov et al., 2017), pagal juos ekspertų vertinimo metodas yra sprendimo teorijos dalis, o pats ekspertų vertinimas yra problemos sprendimo gavimo procedūra sprendimams priimti, vadovaujantis specialistų nuomonėmis. Kelių ekspertų nuomonėmis paremti sprendimai yra tikslesni nei kiekvieno eksperto individuali nuomonė (Burkov et al., 2017). Kartu ekspertas – tai asmuo, kuris dėl savo profesinės arba gyvenimo patirties turi didžiausią kompetenciją ir patikimiausią bei pakankamai išsamią informaciją apie tiriamą problemą (Tidikis, 2003). Taigi, apibendrinant ekspertinio vertinimo metodą, galima teigti, kad šis metodas dažniausiai taikomas norint ištirti ir išspręsti iškeltą problemą ar procesą, kai prireikia specialių gebėjimų bei žinių, o tyrimo rezultatai padeda pateikti objetyvias išvadas ir rekomendacijas.

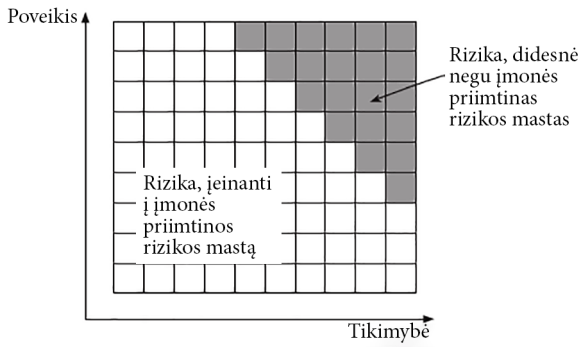
Ekspertinis vertinimas šiame tyrime atliekamas siekiant nustatyti, su kokiais vidiniais bei išoriniais rizikų veiksniais gali susidurti IT įmonė, siekdama pritaikyti *Fintech* įmonės viduje. Ekspertai bus apklausiami žodžiu, vėliau bus vykdomas kiekybinis gautų rezultatų vertinimas. Taip pat jų nuomonių suderinamumas vertinamas Kendall konkordancijos koeficientu W (žr. formulę) (Vitkus et al., 2020).

$$W = \frac{12S}{k^2\left(n^3 - n\right)},$$

čia S – nuokrypio nuo vidutinio rango kvadratų suma; k – ekspertų skaičius; n – pateiktų kriterijų skaičius.

Rizikos žemėlapis, kiekybiniai ir kokybiniai metodai. Bendrovei, siekiančiai atvaizduoti ir grafiškai išreikšti rizikos mastą, tikslui pasiekti gali būti naudojamas rizikos žemėlapis (3 pav.). Sudarant rizikos žemėlapį rizikos tikimybė bus nurodoma horizontalioje ašyje, rizikos poveikis – vertikalioje.

Rizikos žemėlapiai gali būti naudojami tiek siekiant identifikuoti rizikas, tiek siekiant nustatyti rizikos veiksnių prioritetus bei juos įvertinti. Žemėlapiai gali apimti kokybinę ir kiekybinę skalę. Aukščiausia rizika bus matoma žemėlapio dešiniajame, aukščiausiame kampe, mažiausia, priešingame – kairiajame, apatiniame kampe. Pažymima, kad rizikos žemėlapiuose skirtingi rizikos lygiai taip pat gali būti žymimi skirtingomis spalvomis, pvz., žalia, geltona ir raudona,



3 paveikslas. Rizikos žėmėlapis (Martinkutė-Kaulienė ir Stasytytė, 2018)

arba juodos spalvos atspalviais. Bendra taisyklė tokia, kad jei rizikos išsidėsčiusios ryškiame arba tamsiausiame juodos spalvos atspalvyje – tuo įmonė labiau į tas rizikas turėtų reaguoti.

Rizikos analizės ir įvertinimo etapuose taip pat gali būti taikomi kokybiniai ir kiekybiniai metodai. Kokybiniai metodai taikomi, kai riziką sunku nustatyti ar išreikšti kiekybiškai, arba jei įmonė neturi užtektinai duomenų kiekybiniam vertinimui atlikti. Vykdant kiekybinį vertinimą šiame tyrime rizikas galima vertinti matuojant jų bendrą rizikos lygį, kuris išvedamas pagal ekspertų apklausos rezultatus (kai tam tikrai rizikai / įvykiui suteikiama procentinė tikimybės išraiška bei dešimtbalėje sistemoje įvertinamas poveikis). Kokybiniu metodu bus numatytas tikimybės ir pasekmės vertinimas naudojant vertinimo skalę nuo „labai maža“ iki „labai didelė“. Kiekybiniu metodu – tikimybės vertinimas per metus pasikartojusių atvejų skaičiumi ir / arba pasekmės vertinimas specifinių nuostolių skaičiais (Zakabunin, 2014).

3. IT įmonių rizikos tyrimas diegiant *Fintech*

3.1. Ekspertų apklausa

Įmonė, nusprendusi įsidiegti duomenų analizės *Fintech* technologiją bei taip siekianti palengvinti finansinių duomenų analizę, pradeda nuo galimų rizikų identifikavimo. Kaip ir minėta metodikos dalyje, siekiant identifikuoti rizikas, pirmiausia žodžiu atliekama penkių IT įmonės ekspertų – t. y. įmonės direktoriaus, duomenų apsaugos pareigūno, produkto inžinerijos padalinio vadovo, operacinio padalinio vadovo bei klientinių komandų vadovo – apklausa. Taigi, šios ekspertų apklausos tikslas – išsiaiškinti, su kokiomis rizikomis / įvykiais įmonė gali susidurti tiek bendrai, tiek nusprendusi optimizuoti IT procesus bei pradėti naudoti *Fintech*. Ekspertų pasirinkimo kriterijai pateikiami 2 lentelėje.

2 lentelė. Ekspertų pasirinkimas (sudaryta autorės)

Nr.	Pareigų pavadinimas	Išsilavinimas	Darbo patirtis įmonėje (metais)
1	Duomenų apsaugos pareigūnas	Aukštasis	5
2	Įmonės direktorius	Aukštasis	10
3	Produkto inžinerijos padalinio vadovas	Aukštasis	10
4	Operacijų padalinio vadovas	Aukštasis	5
5	Klientinių komandų vadobas	Aukštasis	7

Taigi, 2 lentelėje matoma pasirinktų ekspertų informacija: pareigų pavadinimas, išsilavinimas, darbo patirtis įmonėje. Kad ekspertų suderinamumo rezultatai būtų tikslesni, pasirinkti ekspertai yra įgiję aukštąjį išsilavinimą bei dirba įmonėje daugiau kaip 5 metus.

3.2. SSGG analizė, matrica bei rizikų sąrašas

Iš gautos informacijos apklausos metu toliau sudaryta SSGG analizė (3 lentelė). Šios analizės tikslas yra identifikuoti įmonės stiprybes, silpnybes, galimybes bei grėsmes. Taip pat pažymima, kad 3 lentelėje stiprybės ir silpnybės laikomos vidiniais organizacijos veiksniais, o galimybės ir grėsmės – išoriniais aplinkos veiksniais.

3 lentelė. IT imonės SSGG analizė (sudaryta autorės)

	STIPRYBĖS	SILPNYBĖS
Vidiniai veiksniai	1. Aukšta darbuotojų kompentecija	5. Vidutiniški finansiniai ištekliai
	2. Unikalūs produkto sprendimai	6. Esami įsipareigojimai
	3. Lojalūs klientai	7. Investiciniai įsipareigojimai
	4. Geras technologijos lygis	8. Nėra bendros vizijos
		9. Silpni paskirstymo kanalai
		10. Mažas rinkodaros biudžetas
		11. Greitas technologijos nusidėvėjimas
		12. Automatinių / administracinių procesų trūkumas
		13. Per siaura produktų pasiūla
Išoriniai veiksniai	GALIMYBĖS	GRĖSMĖS
	14. Galimybė skverbtis į naujas rinkas ar rinkos segmentus (įsidiegus *Fintech*)	21. Dėl padidėjusių išlaidų pandemijos metu klientai gali sumažinti savo biudžetus ir nebesinaudoti įmonės teikiamomis paslaugomis
	15. Didenis dėmesys verslo automatizavimui, naujų procesų diegimui	22. Ribota darbo jėgos pasiūla
	16. Papildomos vartotojų grupės	23. Aukšta darbo jėgos migracija
	17. Europos Sąjungos skiriamas finansavimas IT įmonėms	24. Lėtas rinkos augimas
	18. Produktų išplėtimas	25. Nepalankūs valiutų kursai
	19. Produktų diversifikavimas	26. Besikeičiantys pirkėjų norai ir poreikiai
	20. Greitesnis rinkos augimas	27. Nepalankūs demografiniai pokyčiai

Iš anksčiau sudarytos SSGG analizės matomos tokios stiprybės, kaip aukšta darbuotojų kompentecija, unikalūs produkto sprendimai, prie silpnybių priskiriami esami įsipareigojimai, silpni paskirstymo kanalai ir kita. Aptariant galimybes įvardinami tokie veiksniai, kaip produktų išplėtimas, jų diversifikavimas, greitesnis rinkos augimas, o nurodant grėmes matoma, kad jaudinamasi dėl per lėto rinkos augimo, nepalankių valiutų kursų, ribotos darbo jėgos pasiūlos ir kita.

Vadovaujantis SSGG analize, matoma 3 lentelėje, sudaroma 4 lentelė – SSGG matrica, kuri formuluojama pateikiant prioritetines strategijas pagal keturias kategorijas:

– S-GA – pasinaudoti stiprybėmis taip, kad būtų išnaudotos visos galimybės.
– S-GR – pasinaudoti stiprybėmis mažinant grėsmes.
– S'-GA – naudojantis galimybėmis stiprinti silpnybes.
– S'-GR – silpnybes vertinti grėsmių kilimo požiūriu (Martinkutė-Kaulienė & Stasytytė, 2018).

4 lentelė. SSGG matrica (sudaryta autorės remiantis SSGG analize)

	STIPRYBĖS	SILPNYBĖS
GALIMYBĖS	Nr. 1 <-- Nr. 18	Nr. 14 <-- Nr. 5, 9, 13
	Nr. 2 <-- Nr. 14, 16, 17	Nr. 15 <-- Nr. 8, 11, 12, 13
	Nr. 4 <-- Nr. 15, 17	Nr. 16 <-- Nr. 5, 6, 7, 10, 13
		Nr. 17 <-- Nr. 5, 6, 7, 9, 10, 12, 13
		Nr. 18 <-- Nr. 5, 6, 7, 8, 11, 12
		Nr. 19 <-- Nr. 13
		Nr. 20 <-- Nr. 5
GRĖSMĖS	Nr. 1 <-- Nr. 26	Nr. 5 <-- Nr. 23
	Nr. 2 <-- Nr. 21	Nr. 6,7 <-- Nr. 21, 25, 27
	Nr. 3 <-- Nr. 24, 26	Nr. 10, 11, 12, 13 <-- Nr. 24, 26
	Nr. 4 <-- Nr. 21, 26	

Iš pateiktos SSGG matricos matoma, kad tam tikros galimybės, pvz., didesnis dėmesys verslo automatizavimui, naujų procesų diegimui bei Europos Sąjungos skiriamas finansavimas IT įmonėms, puikiai padėtų įmonei pasiekti gerą technologijų lygį. Turimas geras technologijų lygis padėtų sumažinti tokias grėsmes kaip klientų išsaugojimas įmonėje ir kita.

Iš anksčiau sudarytos SSGG matricos bei SSGG analizės toliau sudaromas rizikų sąrašas (5 lentelė), kuris padės identifikuoti veiksnius / priežastis, dėl kurių gali kilti / atsirasti tam tikra rizika.

5 lentelė. Rizikų sąrašas (sudaryta autorės remiantis minčių lietaus (ang. *Brainstorming*) metodu analize bei matrica)

Nr.	Priežastis	Rizika (įvykis)
1	Įdiegta „pasenusi“ technologija	Naujai diegiamos technologijos valdymo sutrikimas
2	Netinkamai/nevisiškai įdiegta technologija	Naujai diegiamos technologijos valdymo neveikimas
3	Atsarginės kopijos/serverio neturėjimas	Duomenų praradimas (įskaitant dalinį duomenų praradimą)
4	Nekompetentingi darbuotojai	Duomenų suklastojimas
5	Duomenų apsaugos nebuvimas/nepakankamumas	Konfidencialių duomenų/informacijos nutekinimas/ paviešinimas
6	Nepakankami finansiniai ištekliai	Didelė personalo kaita
7	Netinkami apmokymo procesai, jų nebuvimas	Ilgai trunkantys apmokymai
8	Nepalankūs demografiniai pokyčiai	Ribota darbo jėgos pasiūla
9	Netinkamai/nevisiškai įdiegta technologija	Kompetencijų trūkumas
10	Prastai ištirta/visiškai neišanalizuota rinka	Naujo proceso/technologijos nenaudojimas
11	Apmokymų nebuvimas, pareiginių nuostatų nebuvimas, infrastruktūros gedimai	Neteisingas duomenų gavimas/perdavimas
12	Per siaura produktų pasiūla, nepakankama darbo jėga	Klientų praradimas
13	Tiekėjo paslaugos neužtikrinimas	Interneto dingimas
14	Netinkamai/nevisiškai įdiegta technologija	Netinkamas duomenų perdavimas kitoms sistemoms (įskaitant trumpą laiko tarpą)
15	Blogi procesai, nėra pareiginių nuostatų	Atsakingo žmogaus nebuvimas/nepaskyrimas
16	Per siaura produktų pasiūla, nepakankama darbo jėga	Klientų praradimas
17	Netinkamas ataskaitų pildymas, darbų neįvykdymas, darbo jėgos sumažėjimas	ES finansavimo netekimas
18	Apmokymų nebuvimas, darbo procesų pasunkinimas	Didžioji dalis darbuotojų nepritaria pasikeitusiam darbų organizavimui
19	Draudimo sąlygų nesilaikymas	Profesinės veiklos draudimo išmokos negavimas
20	Netinkami apmokymai, nekompetentingi darbuotojai	Darbuotojų klaidos
21	Tiekėjo paslaugų trukdžiai	Elektros dingimas
22	Netinkamai/nevisiškai įdiegta technologija	Antivirusinės programos nesuveikimas
23	Nekompetentingi darbuotojai, antivirusinės programos nebuvimas	Kenkėjiškos programinės įrangos įdiegimas per klaidą
24	Netinkamai atrinkti darbuotojai	Tyčiniai veiksmai kenkiantys įmonei
25	Atsakingo darbuotojo už infrastruktūros priežiūrą nebuvimas	Iinfrastruktūros gedimai

Į registrų sąrašą įtraukiamos skirtingos dvidešimt penkios rizikos: naujai diegiamos technologijos valdymo sutrikimas, kuris gali būti netinkamai / nevisiškai įdiegtos technologijos pasekmė, klientų praradimas, lemiamas per siauros produktų pasiūlos, nepakankama darbo jėga, kompetencijų trūkumo rizika, lemiama apmokymų nebuvimo, nepakankamų finansinių išteklių bei kita.

Siekiant nustatyti reikšmingiausias rizikas (įvykius), kurios gali kilti nusprendus įmonei naudoti *Fintech* savo produktuose, procesuose ar jų automatizavimo procese, pagal 5 lentelę toliau sudarytas klausimynas. Šiame klausimyne kiekvienas rizikos punktas buvo ekspertų vertinamas pagal tikimybę (labai maža 0 %; labai didelė 100 %) bei vertinamas tos rizikos poveikis (mažas 1; labai didelis 10), vadovaujantis jų patirtimi įmonėje. Gauti rezultatai matomi 6 lentelėje.

Iš ekspertų apklausos rezultato sandaugos būdu išvedamas rizikos lygis (tikimybė dauginta iš poveikio). Toliau, naudojantis MS *Excel* CORREL funkcija, surandamas labiausiai panašus dviejų ekspertų nuomonių suderinamumas (žr. 6 lentelę).

6 lentelė. Ekspertų nuomonių suderinamumo rezultatai (sudaryta autorės)

Rizikos Nr. (pagal 5 lentelę)	Ekspertas nr. 1 (tikimybė)	Ekspertas nr. 2 (tikimybė)	Ekspertas nr. 3 (tikimybė)	Ekspertas nr. 4 (tikimybė)	Ekspertas nr. 5 (tikimybė)
Ekspertas nr. 1	1,0000	0,9589	0,9881	0,9857	0,9522
Ekspertas nr. 2	0,9589	1,0000	0,9612	0,9801	0,9616
Ekspertas nr. 3	0,9881	0,9612	1,0000	0,9904	0,9598
Ekspertas nr. 4	0,9857	0,9801	0,9904	1,0000	0,9710
Ekspertas nr. 5	0,9522	0,9616	0,9598	0,9710	1,0000

Iš gautų rezultatų matomas, kad tarp daugumos ekspertų yra didelis suderinamumas (koeficientas netoli 1), t. y., didžiausias nuomonių suderinamumas tarp eksperto Nr.3 ir Nr.4 (0,9904) bei tarp Nr. 3 ir Nr. 1 (0,9881).

Suradus labiausiai derančių ekspertų vertinimus, toliau atliekamas visų penkių ekspertų vertinimo suderinamumo lygis, kuris nustatomas pagal konkordacijos koeficientą *W*. Atlikus skaičiavimus pagal Kendall konkordacijos koeficientą *W*, daroma išvada, kad ekspertų atsakymai dera tarpusavyje.

3.3. Kokybinis bei kiekybinis rizikos vertinimas, skirtas didžiausioms rizikoms (įvykiams) nustatyti

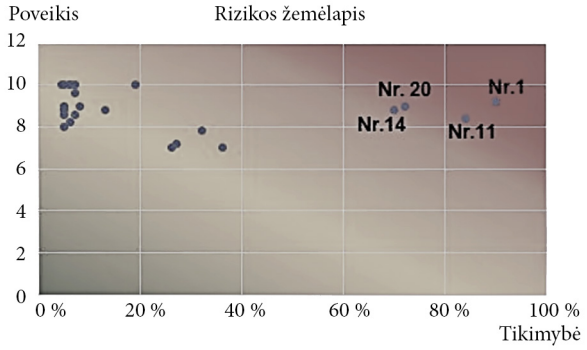
Šio straipsnio teorinėje bei metodologinėje dalyje buvo minima ne tik rizikų identifikavimo svarba, bet ir jų prioritetų / didžiausio poveikio nustatymo reikšmingumas. Remiantis ekspertų apklausa, vertinimų vidurkiu, sandaugos būdu nustatomas rizikos lygis, matomas 7 lentelėje.

7 lentelė. Kokybinis rizikos vertinimas (sudaryta autorės remiantis ekspertų vertinimu)

Nr.	Rizikos lygis pagal Ekspertą nr. 1	Rizikos lygis pagal Ekspertą nr. 2	Rizikos lygis pagal Ekspertą nr. 3	Rizikos lygis pagal Ekspertą nr. 4	Rizikos lygis pagal Ekspertą nr. 5	Bendras rizikos lygis
1	9	8	8	8,1	8,1	8,2
2	0,5	0,5	0,5	1	0,5	0,6
3	0,5	1	0,4	0,45	1,2	0,71
4	0,5	0,5	0,5	0,5	0,5	0,5
5	0,5	0,2	0,5	0,5	0,5	0,44
6	1,8	1,2	2,4	2	2,4	1,96
7	2,4	2,4	2,4	2,4	2,8	2,48
8	2,4	1,8	2,1	1,4	1,4	1,82
9	2,7	1,4	2,4	2,4	3,5	2,48
10	1,5	0,5	0,5	0,5	0,5	0,7
11	7,2	7,2	7,2	7,2	6,4	7,04
12	0,5	0,5	0,4	0,4	0,45	0,45
13	0,35	0,9	0,45	0,45	0,9	0,61
14	5,6	6	5,6	5,6	8	6,16
15	1,2	0,4	2	1	1	1,12
16	0,5	0,4	0,4	0,45	0,5	0,45
17	0,9	0,35	0,45	0,45	0,35	0,5
18	0,4	0,4	0,4	0,4	0,4	0,4
19	0,8	0,5	0,5	0,5	1	0,66
20	8	4,8	7,2	6,3	6,3	6,52
21	0,4	0,4	0,45	0,45	0,45	0,43
22	0,5	0,4	0,45	0,45	0,4	0,44
23	0,5	0,5	0,5	0,5	1	0,6
24	0,5	0,5	1	0,5	0,5	0,6
25	2	1,5	2	2	2	1,9

Atlikus kokybinį vertinimą, matoma, jog bendros rizikos lygis, pagal ekspertų vertinimą yra nuo 0,4 iki 8,2 balo. Tai reiškia, kad pagal gautą rizikos lygį, nurodoma, kad mažiausia reikšmė skiriama baudos gavimo rizikai – 0,4 balai (aštuoniolikta rizika sąraše), o didžiausia – 8,2 balai - suponuoja tikimybę patirti naujai diegiamos technologijos sutrikimus (pirmoji rizika sąraše).

Nustačius rizikos lygį (7 lentelė) bei siekiant vizualiai aiškiau identifikuoti rizikos poveikį bei tikimybę *Excel* programa sukuriamas rizikos žemėlapis (4 pav.).



4 paveikslas. Rizikos žemėlapis (sudaryta autorės remiantis ekspertų vertinimu)

Remiantis rizikos žemėlapio vizualizacija, matoma, kad įmonei, nusprendusiai įsidiegti finansines technologijas, didžiausios galimos rizikos yra naujai diegiamos technologijos valdymo sutrikimas, neteisingų duomenų gavimas/perdavimas bei galimos darbuotojų klaidos. Būtent į prieš tai paminėtas rizikas įmonė turėtų reaguoti stipriausiai ir, jei įmanoma, įsivertinti galimus finansinius nuostolius.

8 lentelė. Kiekybinis rizikos vertinimas (sudaryta autorės remiantis įmonės finansiniais bei konsultantų pateiktais duomenimis)

Nr.	Rizikos (įvykio) kaštai, jei rizikos trukmė 1 mėn.	Tikimybė (%)	DU kaštai (€) (pasirinkti pagal įmonėje prieinamą informaciją)	Pajamų praradimas	Poveikis (€)
1	Naujai diegiamos technologijos valdymo sutrikimas	90 %	4,823	9600	8644
11	Netinkamas duomenų perdavimas kitoms sistemoms	70 %	9,646	14 400	10 087
20	Darbuotojų klaidos (neįskaitant piktybiškų veiksnių)	70 %	5576	4800	7263
14	Neteisingai suvesti duomenys	85 %	7779	11 605	16 476
				Suma	42 470

Atlikus kiekybinį rizikos vertinimą tarp pagrindinių rizikų, matomas skirtingas rizikų finansinis poveikis. Didžiausi nuostoliai galėtų būti patiriami dėl neteisingai suvestų duomenų, sekančiai – dėl netinkamų duomenų perdavimo kitoms sistemoms, naujai diegiamos technologijos valdymo sutrikimo, bei mažiausi nuostoliai būtų patiriami dėl darbuotojų klaidos (neįskaintant piktybiškų veiksnių). Atsižvelgiant į tai, kad įmonės investicija į finansinių technologijų naudojimą ir procesų automatizavimą kol kas siekia 20 000 eurų, o galimų nuostolių suma siekia 42 470 eurų, prieš įgyvendinant projektą bei siekiant išvengti nuostolių ateityje, privaloma minėtas rizikas sumažinti.

4. Rezultatai

Atlikus nagrinėjamos IT įmonės SSGG analizę bei sudarius SSGG matricą matoma, kad įmonė, siekianti pritaikyti *Fintech*, jų procesus bendrovės viduje, gali susidurti su įvairiomis tiek vidinėmis, tiek išorinėmis rizikomis, tokiomis kaip ES finansavimo netekimas, klientų sumažėjimas ar darbuotojų kompetencijų trūkumas ir kita. Pasirinkus ir apklausus penkis ekspertus bei atlikus ekspertinį vertinimą, preziumuojama, kad ekspertai pasirinkti teisingai ir jų vertinimai yra suderinami (*W* koeficientas = 0,9904). Atlikus kokybinį rizikos vertinimą (remiantis ekspertų apklausa bei nubraižius

rizikos žemėlapį) daroma išvada, kad rizikos / įvykiai, kurie gali daryti didžiausią įtaką Fintech procesų naudojimui, yra naujai diegiamos technologijos valdymo sutrikimas, neteisingų duomenų gavimas/perdavimas bei galimos darbuotojų klaidos. Apžvelgus anksčiau gautus rezultatus buvo nuspręsta atlikti kiekybinį pirmųjų didžiausių 4 rizikų vertinimą (8 lentelė), kuris tik įrodė, jog įmonė, prieš diegdama naujus *Fintech* procesus, privalo imtis reikalingų priemonių, kurios būtų tinkamas atsakas į galimas rizikas (vengti, mažinti, pasidalinti ar prisiimti). Priešingu atveju įmonei gresia nuostoliai, kurie sudėjus pagrindines rizikas gali siekti net 42 470 eurų sumą. Įmonei, turinčiai tiek kokybinį, tiek kiekybinį rizikos vertinimą, toliai reikėtų nuspręsti, kurias rizikas turėtų mažinti greičiausiai.

Išvados

Remiantis apžvelgtais moksliniais darbais, daroma išvada, kad rizika ir rizikos valdymas yra neatskiriami dalykai kalbant apie verslą, jo vykdymą bei tobulinimą. Rizikos gali kilti tiek iš išorės, tiek iš įmonės vidaus veiksnių. IT imonė, siekianti įsidiegti bendrovės viduje *Fintech*, gali susidurti su tokiomis rizikomis kaip likvidumo, duomenų saugumo, rinkos, operacinės bei kredito.

Šiame tyrime nuspręsta vadovautis ISO valdymo standartais (atliekamas rizikos identifikavimas, rizikos analizė bei rizikos įvertinimas). Siekiant identifikuoti galimas rizikas, buvo atlikta ekspertų apklausa, panaudotas daugiakriteris vertinimo metodas SAW bei patikrintas ekspertų vertinimo suderinamumas. Iš gautų duomenų sudaryta SSGG analizė bei matrica, kuri leido identifikuoti galimas rizikas siekiant pasinaudoti *Fintech*.

Atlikus kiekybinį bei kokybinį rizikos vertinimą remiantis ekspertų apklausa bei nubraižius rizikos žemėlapį daroma išvada, kad rizikos / įvykiai, kurie gali daryti didžiausią įtaką *Fintech* procesų naudojimui, naujai diegiamos technologijos valdymo sutrikimas, neteisingų duomenų gavimas/perdavimas bei galimos darbuotojų klaidos. Darbe taip pat nustatyta, kad nustačius potencialias rizikas, tinkamai jas įvertinus bei nustačius jų poveikio lygį, norint, kad rizikos valdymas būtų veiksmingas bei kuo mažiau sumažintų galimas grėsmes, įmonė privalo imtis reikalingų priemonių, kurios būtų tinkamas atsakas į galimas rizikas (t. y. rizikų galima vengti, jas mažinti, pasidalinti ar prisiimti), priešingu atveju įmonė gali patirti 42 470 eurų sumos nuostolius.

Be visa to, svarbu pabrėžti, kad šiame straipsnyje nagrinėta viena IT įmonė bei pasitelkti 5 įmonės ekspertai, kurie padėjo įvertinti *Fintech* proceso riziką siekiant ją įsidiegti bendrovėje. Norint dar geriau įvertinti galimas *Fintech* rizikas IT įmonėje ateityje nagrinėjamų IT įmonių skaičius didės, kaip ir pasitelktų ekspertų skaičius, siekiant atlikti rizikos vertinimą. Visa tai padėtų gauti dar tikslingesnius rezultatus.

Literatūra

Ancri, C. (2016). *Fintech innovation: An overview*. https://www.cbinsights.com/blog/disrupting-banking-Fintech-startups/

Arner, D., Barberis, J., & Buckley, R. (2015). *The evolution of Fintech: A new post-crisis paradigm*? (Research Paper No. 2015/047). University of Hong Kong Faculty of Law. https://doi.org/10.2139/ssrn.2676553

Baker McKenzie. (2020). *Top 10 op risks 2020*. Risk.Net. https://www.eurasiagroup.net/files/upload/Top_Risks_2020_Report_1.pdf

Burkov, E. A., Lyubkin, P. L., & Paderno, P. I. (2017). Intellectual systems – the future of expert assessment. In *XX IEEE International Conference on Soft Computing and Measurements (SCM)*, pp. 34–36. https://doi.org/10.1109/SCM.2017.7970487

Chanias, S., Myers, M. D., & Hess, T. (2019). Digital transformation strategy making in pre-digital organizations: The case of a financial services provider. *Journal of Strategic Information Systems*, *28*(1), 17–33. https://doi.org/10.1016/j.jsis.2018.11.003

Chen, M. A., Wu, Q., & Yang, B. (2019). How valuable is FinTech innovation? *Review of Financial Studies*, *32*(5), 2062–2106. https://doi.org/10.1093/rfs/hhy130

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise risk management – Integrated Framework*. COSO. https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

Dadelytė, E., & Mačiulytė-Šniukienė, A. (2019). Banko sektoriaus veiklos efektyvumo vertinimas. Iš *22-osios Lietuvos jaunųjų mokslininkų konferencijos „Mokslas – Lietuvos ateitis“ teminė konferencija, Ekonomika ir vadyba / Economics and Management*. 2019 m. vasario 13 d. Vilnius.

Dhar, V., & Stein, R. M. (2017). Fintech platforms and strategy. *Communications of the ACM*, *60*(10), 32–35. https://doi.org/10.1145/3132726

Edirisinghe Vincent, N., & Pinsker, R. (2020). IT risk management: Interrelationships based on strategy implementation. *International Journal of Accounting and Information Management*, *28*(3), 553–575. https://doi.org/10.1108/IJAIM-08-2019-0093

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the Fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems*, *35*(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766

Heidary Dahooie, J., Razavi Hajiagha, S. H., Farazmehr, S., Zavadskas, E. K., & Antucheviciene, J. (2021). A novel dynamic credit risk evaluation method using data envelopment analysis with common weights and combination of multi-attribute decision-making methods. *Computers and Operations Research*, *129*, 105223. https://doi.org/10.1016/j.cor.2021.105223

Hynes, C. (2018). *Latest Fintech solutions to improve your business efficiency*. https://www.eastwestbank.com/ReachFurther/en/News/Article/Latest-Fintech-Solutions-to-Improve-Your-Business-Efficiency

Hu, Z., Ding, S., Li, S., Chen, L., & Yang, S. (2019). Adoption intention of Fintech services for bank users: An empirical examination with an extended technology acceptance model. *Symmetry*, *11*(3), 340. https://doi.org/10.3390/sym11030340

International Organization of Standardization. (2009). *Risk management – principles and guidelines* (ISO 31000:2009). Geneva, Switzerland.

Janeliūnienė, R. ir Davidavičienė, V. (2013). IT rizikos identifikavimo proceso analizė. *Mokslas – Lietuvos Ateitis*, *5*(1), 46–52. https://doi.org/10.3846/mla.2013.07

Jevsejev, R. (2020). Information technology risk assessment methods and improvement solutions. *Mokslas – Lietuvos Ateitis*, *12*, 1–7. https://doi.org/10.3846/mla.2020.10562

Kahraman, C., Ruan, D., & Dogan, I. 2018. Fuzzy group decision-making for facility location selection. *Information Sciences*, *157*, 135–153. https://doi.org/10.1016/S0020-0255(03)00183-X

Keong, O. C., Leong, T. K., & Bio, C. J. (2020). Perceived risk factors affect intention to use Fintech. *Journal of Accounting and Finance in Emerging Economies*, *6*(2), 453–463. https://doi.org/10.26710/jafee.v6i2.1101

Kovacs, O. (2018). The dark corners of industry 4.0 – Grounding economic governance 2.0. *Technology in Society*, *55*, 140–145. https://doi.org/10.1016/j.techsoc.2018.07.009

Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, *61*(1), 35–46. https://doi.org/10.1016/j.bushor.2017.09.003

Lee, Y. H. (2013). Application of a SWOT-FANP method. *Technological and Economic Development of Economy*, *19*(4), 570–592. https://doi.org/10.3846/20294913.2013.837111

Lietuvos Respublikos finansų ministerija. (2020). *Lietuva – Fintechrinkos lyderė Europos Sąjungoje 2020*. https://finmin.lrv.lt/lt/naujienos/lietuva-finansiniu-technologiju-rinkos-lydere-europos-sajungoje

Manta, O. (2018). Financial technologies (fintech), instruments, mechanisms and financial products. *Internal Auditing Risk Management*, *52*(4), 78–102.

Martinkutė-Kaulienė, R. ir Stasytytė, V. (2018). *Rizikos valdymas: vadovėlis*. Technika. https://doi.org/10.20334/2018-008-S

Moghni, H., Nassehifar, V., & Nategh, T. (2020). Designing model for quality services in digital banking. *Journal of Critical Reviews*, *7*(9), 679–690. https://doi.org/10.31838/jcr.07.09.132

Rutkauskas, A. V. ir Stasytytė, V. (2011). Rizikos sampratos formavimosi ypatumai. *Verslas: teorija ir praktika*, *12*(2), 141–149. http://dx.doi.org/10.3846/btp.2011.15

Ryu, H.-S. (2018). Understanding benefit and risk framework of fintech adoption: Comparison of early adopters and late adopters. In *Proceedings of the 51st Hawaii International Conference on System Sciences. Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2018.486

Schattenberg, M., Heymann, E., Schneider, S., & Korner, K. (2018). *Digital Economics – How AI and Robotics are chenging our work and our lives*. EU Monitor.

Schwab, K. (2016). *The Fourth industrial revolution: What it means, how to respond.* World Economic Forum.

Serikoviene, S. (2013). *Mokomųjų objektų daugkartinio panaudojamumo kokybės vertinimo metodų taikymo tyrimas* (Daktaro disertacija). https://www.mii.lt/files/doc/lt/doktorantura/apgintos_disertacijos/mii_dis_2013_serikoviene.pdf

Stasytytė, V., & Aleksienė, L. (2015). Operational risk assessment and management in small and medium-sized enterprises. *Business: Theory and Practice*, *16*(2), 140–148. https://doi.org/10.3846/btp.2015.568

Sweeney, D. (2017). *What does Fintech mean for SMBs*. Retrieved October 7, 2019, from https://www.business.com/articles/what-is-Fintech-and-what-does-it-mean-for-small-businesses/

Tabasi, H., Yousefi, V., Tamošaitienė, J., & Ghasemi, F. (2019). Estimating conditional value at risk in the Tehran stock exchange based on the extreme value theory using GARCH models. *Administrative Sciences*, *9*(2), 40. https://doi.org/10.3390/admsci9020040

Thakor, A. V. (2020). Fintech and banking: What do we know? *Journal of Financial Intermediation*, *41*, 100833. https://doi.org/10.1016/j.jfi.2019.100833

Tidikis, R. (2003). *Socialinių mokslų tyrimų metodologija: vadovėlis*. Lietuvos teisės universiteto Leidybos centras.

Varga, D. (2017). Fintech, the new era of financial services. *Vezetéstudomíny-Budapest Management Review*, *48*(11), 22–32. https://doi.org/10.14267/VEZTUD.2017.11.03

Vitkus, D., Salter, J., Goranin, N., & Čeponis, D. (2020). Method for attack tree data transformation and import into IT risk analysis expert systems. *Applied Sciences* (Switzerland), *10*(23), 8423. https://doi.org/10.3390/app10238423

IT COMPANY RISK ASSESSMENT IN IMPLEMENTATION OF FINANCIAL TECHNOLOGIES

Augustina DUMPYTĖ, Indrė LAPINSKAITĖ

Abstract. Nowadays, the focus on financial technologies and their processes is increasing. Financial technology is recognized as one of the most important innovations in the financial industry, which is developing extremely rapidly. Consenquely, not only financial sectory is using these new technologies. Financial technologies can be adapted by information technology (IT) companies. The article reveals the essence and content of the Fintech concept and formulates the main types of financial technology innovation. It also analyzes the risks that IT companies may face when deciding to implement financial technologies internally. The main goal of this study is to examine the possible risks of Fintech implementation/process used, to perform their assessment in IT companies. To achieve the goal, the analysis and systematization of scientific literature sources, expert surveys, quantitative and qualitative assessments, SWOT analyses, risk map are used. The purpose of this article is to reveal what risks Fintech needs to know and assess in order to effectively implement technologies in IT companies. In conclusion, results agree with mentioned hypothesis.

Keywords: financial technologies, financial technology risk and assessment, risk evaluation, information technology.