VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
TRANSPORTO INŽINERIJOS FAKULTETAS
LOGISTIKOS IR TRANSPORTO VADYBOS KATEDRA

Rūta Vilkoicaitė

BIOMETRINIŲ TECHNOLOGIJŲ TAIKYMO LOGISTIKOS PROCESAMS GERINTI TYRIMAS
STUDY OF THE APPLICATION OF BIOMETRIC TECHNOLOGIES FOR THE IMPROVEMENT OF LOGISTIC PROCESSES

Baigiamasis magistro darbas

Transporto inžinerinės ekonomikos ir logistikos studijų programa,
valstybinis kodas 6211LX057
Transporto logistikos specializacija
Verslo studijų kryptis

Vilnius, 2024

Vilniaus Gedimino technikos universitetas
Transporto inžinerijos fakultetas
Logistikos ir transporto vadybos katedra

ISBN | ISSN
Egz. sk. .....
Data .....-.....-.....

Antrosios pakopos studijų **Transporto inžinerinės ekonomikos ir logistikos** programos magistro baigiamasis darbas	
Pavadinimas	**Biometrinių technologijų taikymo logistikos procesams gerinti tyrimas**
Autorius	**Rūta Vilkoicaitė**
Vadovas	**Kristina Čižiūnienė**

Kalba: lietuvių

Anotacija

Baigiamajame magistro darbe nagrinėjamos biometrinės technologijos, jų panaudojimo galimybės logistikos srityje, siekiant sudaryti biometrinių technologijų pritaikomumo logistikos srityje modelį, kuris padės užtikrinti kokybišką, saugų ir patikimą darbą. Darbe atlikta mokslinės literatūros analizė, ji padėjo apžvelgti biometrines technologijas teoriniu aspektu. Norint išsamiau įvertinti biometrinių technologijų panaudojimo galimybes logistikos srityje, atliktas kiekybinis ir kokybinis tyrimas. Kokybinio tyrimo rezultatai buvo pritaikyti DEMATEL metodo atlikimui, kuris leido išskirti pačius svarbiausius biometrinių technologijų logistikos srityje komponentus. Atlikus mokslinių šaltinių analizę, anketinę apklausą bei ekspertinį interviu, sudarytas modelis, parodantis biometrinių technologijų integraciją į logistikos procesus. Pateikiamos darbo išvados ir pasiūlymai.

Darbą sudaro: įvadas, 3 skyriai, išvados, siūlymai, literatūros sąrašas ir priedai.

Darbo apimtis – 64 p. teksto, be priedų, 9 paveikslai, 15 lentelių, 63 bibliografiniai šaltiniai.

Prasminiai žodžiai: Reikšminiai žodžiai: logistika, tiekimo grandinė, biometrinės technologijos, identifikavimas, saugumas.

Vilnius Gediminas Technical University
Faculty of Transport Engineering
Logistics and Transport Management Department

ISBN
ISSN
Copies No. .....
Date .....-.....-.....

Master Degree Studies **Transport Engineering Economics and Logistics** study programme Master Graduation Thesis	
Title	**Study of the application of biometric technologies for the improvement of logistic processes**
Author	**Rūta Vilkoicaitė**
Academic supervisor	**Kristina Čižiūnienė**

Thesis language: Lithuanian

Annotation

The final master thesis examines biometric technologies and their potential applications in logistics, with the aim of developing a model for the applicability of biometric technologies in logistics that will help to ensure a high quality, safe and reliable work. The thesis analyses the scientific literature and provides an overview of biometric technologies from a theoretical point of view. In order to further assess the applicability of biometric technologies in logistics, a quantitative and qualitative study was carried out. The results of the qualitative study were applied to the DEMATEL approach, which allowed the identification of the most important components of biometric technologies in logistics. The analysis of scientific sources, a questionnaire survey and an expert interview led to the construction of a model showing the integration of biometric technologies into logistics processes. Conclusions and suggestions are presented.

The thesis consists of: introduction, 3 chapters, conclusions, suggestions, list of references and annexes.

The thesis consists of 64 pages of text, excluding appendices, 9 figures, 15 tables, 63 bibliographical references.

Keywords: Keywords: logistics, supply chain, biometric technologies, identification, security.

TURINYS

PAVEIKSLŲ SĄRAŠAS 5
LENTELIŲ SĄRAŠAS 5
SANTRUMPŲ SĄRAŠAS 6
ĮVADAS 7
1. BIOMETRINIŲ TECHNOLOGIJŲ ANALIZĖ TEORINIU ASPEKTU 9
1.1. Biometrinių technologijų samprata 9
1.2. Biometrinių technologijų rūšys ir jų veikimo principai 13
1.3. Biometrinių technologijų panaudojimo sritys ir galimybės 20
1.4. Biometrinių technologijų taikymas logistikos procesuose 24
1.5. Teorinės analizės apibendrinimas 28
2. LOGISTIKOS PROCESŲ TOBULINIMO PANAUDOJANT BIOMETRINES TECHNOLOGIJAS TYRIMO METODIKA 31
2.1. Empirinio tyrimo metodologija 31
2.2. Tyrimo metodai ir eiga 32
2.3. Tyrimo duomenų rinkimo organizavimas ir imtis 33
2.4. Kiekybinio tyrimo rezultatai 39
2.5. Kokybinio tyrimo rezultatai 42
2.6. Tyrimų apibendrinimas 47
3. LOGISTIKOS PROCESŲ TOBULINIMO MODELIS PANAUDOJANT BIOMETRINES TECHNOLOGIJAS 49
3.1. Siūlomas modelis 49
3.2. Modelio aprobavimas 52
IŠVADOS 54
SIŪLYMAI 56
LITERATŪROS SĄRAŠAS 57
PRIEDAI 62

PAVEIKSLŲ SĄRAŠAS

1 pav. Biometrinių technologijų rūšys (sudaryta darbo autorės) 16
2 pav. Teorinis modelis (sudaryta darbo autorės) 28
3 pav. Biometrinių technologijų poveikis (sudaryta darbo autorės) 29
4 pav. Biometrinių technologijų naudojimas (sudaryta darbo autorės) 39
5 pav. Saugiausios biometrinės technologijos (sudaryta darbo autorės) 40
6 pav. Biometrinių technologijų panaudojimo sritys (sudaryta darbo autorės) 41
7 pav. Komponentų priežastiniai ir pasekmių ryšiai (sudaryta darbo autorės) 46
8 pav. Strateginis žemėlapis, kuris rodo ryšius tarp komponentų (sudaryta darbo autorės) 48
9 pav. Modelis, rodantis biometrinių technologijų integraciją į logistikos procesus (sudaryta darbo autorės) 50

LENTELIŲ SĄRAŠAS

1 lentelė. Biometrinių technologijų samprata (sudaryta darbo autorės) 10
2 lentelė. 3 pagrindinių identifikavimo būdų privalumai ir trūkumai (Faundez-Zanuy, 2006) 12
3 lentelė. Biometrinių technologijų rūšių privalumai ir trūkumai (sudaryta darbo autorės) 17
4 lentelė. Biometrinių technologijų rūšių savybės (sudaryta darbo autorės) 18
5 lentelė. Pagrindinių biometrinių technologijų rūšių tikslumas ir naudojimas (Dovydaitis, 2018) 23
6 lentelė. Reikšmės imties dydžiui nustatyti (su 5 % paklaida) (Galatiltytė, 2022) 34
7 lentelė. Priežastinių ryšių vertinimo balai (sudaryta darbo autorės) 36
9 lentelė. Pusiau struktūrizuoto ekspertinio interviu ekspertų charakteristikos (sudaryta darbo autorės) 38
10 lentelė. Vieno iš ekspertų atliktas rangavimas (sudaryta darbo autorės) 43
11 lentelė. Susisteminti ekspertų vertinimai (sudaryta darbo autorės) 43
12 lentelė. Tiesioginio ryšio matrica X (sudaryta darbo autorės) 44
13 lentelė. Bendro ryšio matrica T (sudaryta darbo autorės) 44
14 lentelė. Matrica T su apskaičiuotomis R ir C reikšmėmis (sudaryta darbo autorės) 45
15 lentelė. R+C ir R-C reikšmės (sudaryta darbo autorės) 45

SANTRUMPŲ SĄRAŠAS

DEMATEL – sprendimų priėmimo bandymų ir vertinimo laboratorija (angl. *Decision making trial and evaluation laboratory*);

DNR – deoksiribonukleorūgštis (angl. *Deoxyribonucleic acid*);

FTB – Federalinis tyrimų biuras (angl. *Federal Bureau of Investigation*);

ID – asmens tapatybės kortelė (angl. *Identity document*);

MCDM – daugiakriterė sprendimų priėmimo sistema (angl. *Multiple Criteria Decision Making*);

PIN – asmeninis identifikavimo numeris (angl. *Personal identification number*);

RFID – radijo dažnio identifikavimas (angl. *Radio frequency identification*).

ĮVADAS

Darbo aktualumas. Šiuo metu moderniosios technologijos užima svarbią vietą pasaulyje. Turbūt retas įsivaizduoja gyvenimą be telefonų ar kompiuterių. Technologijos ir inovacijos yra pagrindiniai verslo konkurencijos veiksniai. Technologijos palengvina gyvenimą, padeda sutaupyti laiko, didinti pelną bei darbo našumą, tiksliau ir taisyklingiau jį atlikti. Viena iš moderniųjų technologijų rūšių yra biometrinės technologijos – tai asmenų atpažinimas pagal jų unikalius fiziologinius (pirštų atspaudų, veido, rainelės ir kt.) arba elgsenos (balso, eisenos, parašo ir kt.) požymius (Unar et al., 2014). Biometrinės technologijos sukuria didesnį pranašumą prieš kitas sistemas, nes padeda užtikrinti didesnį saugumą ir sumažinti žmogiškojo faktoriaus klaidas. Biometriniai duomenys, pavyzdžiui, tokie kaip balso (Alsaadi, 2021), veido, pirštų (Gayathri et al., 2020), rainelės nuskaitymas (Gomez-Barrero et al., 2022) ir kitos charakteristikos, užtikrina patikimą ir didesnį saugumo lygį tiek asmeniniam, tiek viešajam naudojimui. Norint užtikrinti didesnį saugumą, autentifikavimui galima naudoti multimodalinį junginį (Thenuwara et al., 2022), t. y. sujungti kelias biometrinių technologijų rūšis arba kartu naudoti su kitomis kodinėmis arba RFID sistemomis. Kuo toliau, tuo dažniau biometrinės technologijos pakeičia slaptažodžius asmeninio naudojimo tikslams, viešajame sektoriuje, privačiajame sektoriuje, tyrimų laboratorijose ir panašiai. Taip pat biometrinės technologijos gali būti integruojamos su kitomis logistikos sistemomis, pavyzdžiui, krovinių sekimo sistemomis.

FTB kiekvienais metais renka duomenis apie krovinių vagystes. Remiantis jų duomenimis, kiekvienais metais yra prarandama daugiau kaip 30 mlrd. eurų vertės krovinių, tačiau kiekvienais metais didėjant krovinių kiekiui, daugėja ir krovinių vagysčių (FBI, 2006). Plačiau naudojant biometrines technologijas logistikos procesuose, galima sumažinti krovinių vagysčių atvejus. Numatoma, kad pasaulyje biometrinių technologijų rinka turės 17,06 % metinį augimą iki 2025 m. (Mason et al., 2020).

Darbo problema. Logistikos įmonės siekia efektyvinti ir optimizuoti logistikos procesus, tačiau dažnai susiduria su trikdžiais visoje tiekimo grandinėje dėl žmogiškojo faktoriaus klaidų ar dėl kitų technologijų, pavyzdžiui, RFID, kurios negali užtikrinti tinkamo tikslumo ir saugumo. Problema yra tai, kad logistikos srityje nėra plačiai nagrinėjamas išmaniųjų technologijų panaudojimas, kai išmanūs jutikliai gali padėti realiuoju laiku stebėti ir apdoroti duomenis. Kaip alternatyva naudojamoms technologijoms galėtų būti biometrinės technologijos, tačiau šiuo metu šių technologijų panaudojimas – pavieniai atvejai.

Darbo objektas. Biometrinės technologijos logistikos procesuose.

Darbo tikslas. Sudaryti biometrinių technologijų pritaikomumo logistikos srityje modelį, siekiant užtikrinti kokybišką, saugų ir patikimą darbą.

Šiam tikslui pasiekti keliami **uždaviniai**:

1. Išanalizuoti mokslinę literatūrą biometrinių technologijų teoriniais aspektais.
2. Atlikti tyrimą, siekiant išsiaiškinti logistinių procesų gerinimą panaudojant biometrines technologijas.
3. Pateikti logistikos procesų gerinimo modelį.

Darbo naujumas. Logistikos srityje šios technologijos yra naujovė, visame pasaulyje dar nedaug įmonių savo logistikos procesuose naudoja biometrines technologijas. Biometrinių technologijų panaudojimas yra reikšmingas, nes padeda užtikrinti didesnį saugumą, realiuoju laiku stebėti ir apdoroti duomenis. Biometrinės technologijos užtikrina didesnę apsaugą ir leidžia sistemingai vertinti logistikos procesus, tokius kaip sandėliavimas, transportavimas ar informacijos apdorojimas.

Hipotezė. Biometrinės technologijos didina saugumo lygį ir padeda išlaikyti sėkmingai veikiančius tiekimo grandinės procesus.

Tyrimo metodai: mokslinės literatūros analizė, kiekybinis duomenų rinkimas anketinės apklausos analizės būdu, kokybinis vertinimas interviu būdu, DEMATEL metodas.

1. BIOMETRINIŲ TECHNOLOGIJŲ ANALIZĖ TEORINIU ASPEKTU

1.1. Biometrinių technologijų samprata

Šiuo metu moderniosios technologijos turi didelę reikšmę, jos supaprastina įvairius dalykus ir pagreitina darbus. Išmaniosios technologijos yra sparčiai pažengusios ir nuolatos tobulinamos, kad labiau atitiktų vartotojų poreikius. Naudojant išmaniąsias technologijas, galima pagerinti finansinius rezultatus, išlaikyti stipresnę poziciją rinkoje ir sumažinti sąnaudas. Viena iš moderniųjų technologijų rūšių yra biometrinis duomenų atpažinimas.

Biometrinis duomenų atpažinimas – automatinis asmenų autentifikavimas arba identifikavimas pagal jų unikalius fizinius ar elgesio bruožus (Alsaadi, 2021). Biometrinės technologijos vis plačiau naudojamos pasaulyje, jos apima įvairius žmogaus biometrinius duomenis, pavyzdžiui, pirštų atspaudų skenavimą, rainelės ir tinklainės nuskaitymą, balso, veido atpažinimą ir panašiai. Biometrinis įrenginys skenuoja šiuos biometrinius duomenis tam, kad galėtų atpažinti ir identifikuoti asmenį, o netinkamus duomenis atmesti ir blokuoti tolimesnę prieigą. Nesvarbu, ar šios technologijos naudojamos atskirai, ar kartu, jos taikomos įvairiose aplinkose, siekiant nuskaityti kūno bruožus, nustatyti, patikrinti ir suskirstyti į kategorijas (Grünenberg et al., 2022). Šios technologijos užtikrina didesnį saugumą, tikslumą, padeda labiau sumažinti žmogiškojo faktoriaus klaidas nei RFID ar ranka suvedinėjamus slaptažodžius. Biometrines technologijas sunku suklastoti, kadangi kiekvienas žmogus turi individualius biometrinius duomenis. Net dvynių, kurie atrodo labai panašūs, biometriniai duomenys pasižymi skirtingomis struktūromis ir raštais. Biometrinės technologijos dažniausiai naudojamos automatiniam asmens autentifikavimui, asmens tapatybės nustatymui, siuntų apsaugojimui bei sekimui, todėl jos palengvina ir pagreitina darbą.

Svarbu suprasti ir apibrėžti biometrinių technologijų sampratą bei kur jos gali būti taikomos. Terminas „biometrija“ yra išvestas iš graikų kalbos žodžių „bios“ (gyvybė) ir „metron“ ar „metrikos“ (matas) (Savickas, 2008). Išanalizavus biometrinių technologijų sampratas nuo 2005 m., galima teigti, kad visi analizuoti autoriai aprašo jas panašiai, netgi vienas kitą papildo (žr. 1 lentelę). Pateiktų sampratų analizė rodo, kad Lietuvos ir užsienio autoriai biometrinių technologijų sąvoką apibrėžia gana panašiai – kaip žmogaus individualių bruožų atpažinimo metodą, kuris remiasi asmens fizinėmis ar elgesio savybėmis. Biometrinių technologijų sampratos yra susijusios tarpusavyje su asmens tapatybės atpažinimu, autentifikacija ir identifikacija.

1 lentelė. Biometrinių technologijų samprata (sudaryta darbo autorės)

Biometrinių technologijų samprata	Autorius, metai
Atpažinimo sistema, kuri veikia renkant biometrinius duomenis iš žmonių. Iš gautų duomenų išskiriant funkcijų rinkinį ir lyginant su duomenų bazėje esančiu šablonu.	(Jain, 2005)
Technologijų sritis, kurioje žmogus yra identifikuojamas, tikrinamas arba analizuojamas pagal jo fizinius arba elgsenos biometrinius duomenis.	(Kaklauskas & Zavadskas, 2010)
Technologijų visuma, kurios yra susijusios su asmens tapatybės identifikacija pagal unikalius žmogaus biometrinius duomenis.	(Trukšina & Vasiliauskas, 2014)
Individualių bruožų atpažinimas, remiantis viena ar keliomis vidinės anatomijos, fiziologinėmis ir elgesio savybėmis.	(Bartkienė, 2014)
Žmogaus nuskaitymas naudojant fizines ir elgesio savybes.	(Mason et al., 2020)
Automatinis asmenų atpažinimas, pagrįstas jų biologinėmis savybėmis, tokiomis kaip pirštų atspaudai, rainelė, veidas, venos ir kt., arba elgesio ypatybėmis, tokiomis kaip balsas, parašas, ėjimas.	(Alrahawe et al., 2021)
Technologijos, naudojančios skaitmeninius kūno charakteristikų atvaizdus asmenų tapatybei nustatyti.	(Grünenberg et al., 2022)

Taikant biometrinio identifikavimo metodą, sistema nereikalauja tapatybės, o pati nustato vartotoją. Jei asmuo priklauso iš anksto nustatytam vartotojui, tai vadinama identifikavimu (Faundez-Zanuy, 2006). Identifikavimo metu, reikalinga išorinė duomenų bazė, kurioje identifikavimo metu sutikrinama informacija ar yra suvestas asmuo. Pavyzdžiui, piršto atspaudo nuskenavimas ant skaitytuvo, vardo pateikimas prisijungimo ar įėjimo metu. Tačiau, kai vyksta identifikavimas, asmuo savo duomenų nekontroliuoja, nes jie yra duomenų bazėje, todėl gali kilti asmens duomenų pavojus.

Naudojant identifikavimo metodą, pirmiausiai paimami asmens tam tikri biometriniai duomenys ir atliekamas etaloninis modelis. Su sudarytu modeliu būna lyginami asmens biometriniai duomenys (*Biometrics: Definition, Use Cases, Latest News*, 2021).

Biometriniai duomenys gali būti ne tik laikomi duomenų bazėse, bet ir integruotos į standartinio dydžio korteles ar kitus decentralizuotus įrenginius, kurie užtikrina dar didesnį saugumą ir patogumą (Hussain et al., 2017). Autentifikavimo metodo tikslas – nustatyti, ar asmuo yra tas, kuris teigia esąs. Vartotojas turi pateikti savo tapatybę (Faundez-Zanuy, 2006). Intelektualioji kortelė gali būti naudojama keliems tikslams: autentifikavimui, duomenų saugojimui ir apdorojimui, o jeigu kortelė būtų pamesta ar pavogta, biometrinių duomenų atkurti nepavyktų (Elhennawy & Amer, 2017). Biometrinis autentifikavimas padeda palyginti asmens biometrinius duomenis su to paties žmogaus biometrinėmis savybėmis, kad įrenginys galėtų atpažinti panašumus (*Biometrics: Definition, Use Cases, Latest News*, 2021). Pavyzdžiui, jungiantis prie elektroninio pašto iš kito išmaniojo įrenginio, paprašoma pačiame pašte įrodyti savo tapatybę arba prisijungimo metu yra pateikiamas slaptažodis.

2 lentelėje yra pateikiami 3 pagrindinių identifikavimo ir autentifikavimo būdų privalumai bei trūkumai. RFID kortelės, pasai ir pan. turi stiprų minusą, kad šias laikmenas yra lengva pamesti, pavogti, sugadinti ar net suklastoti. Pavyzdžiui, asmens dokumentai dažnai perkami ir klastojami, jomis nesunkiai gali pasinaudoti kitas neteisėtas asmuo. Šias korteles, pametus ar sugadinus, nesunkiai galima atkurti ir išduoti naujas. Jas lengva nešioti, galima įsidėti į bet kurią patogią vietą, nes jos yra plonos ir mažos. Kitas autentifikavimo būdas – slaptažodžiai ir PIN kodai. Šiais kodais paprasta naudotis, naudojimuisi nereikia jokių specialių įrenginių, o pamiršus, nesunkiai galima pakeisti nauju. Sunku sugalvoti slaptažodžius, kurie būtų stiprūs ir sunkiai pamirštami. Dėl to dažniausiai žmonės galvoja slaptažodžius su augintinių ar gyvenamosios gatvės pavadinimais, kuriuos lengva atspėti ar nulaužti. Šiuo metu yra rekomenduojami stiprūs slaptažodžiai, kuriuos sudarytų ne tik raidės, bes ir skaičiai su simboliais, tačiau sunku sugalvoti lengvai įsimenamą, bet ir saugų slaptažodį, kuris su laiku nepasimirš. Biometrinės technologijos užtikrina, kad teikiamas paslaugas galėtų pasiekti tik tam tikras asmuo. Norint identifikuoti žmogų, yra tikrinami biometriniai duomenys, tokie kaip: žmogaus balsas, veidas, pirštų atspaudai, delno geometrija, parašas, eisena, akies rainelė, tinklainė ir panašiai. Šiuos biometrinius žmogaus duomenis nuskaito skirtingi įrenginiai, tokie kaip vaizdo kameros, fotoaparatai, įvairūs skaitytuvai, kurie skirti nuskaityti pirštų atspaudus, rainelę, veidą, eiseną ir t. t. Kiekvienų biometrinių duomenų skenavimui yra naudojami skirtingi biometriniu duomenis palaikantys įrenginiai (Jurgilas, 2021). Biometrines technologijas paprasta ir patogu naudoti, nes nereikia nešiotis ar atsiminti jokių slaptažodžių. Biometriniai nuskaitymai veikia greitai ir saugiai, nes kiekvieno žmogaus biometriniai duomenys yra unikalūs.

Tam tikriems biometrinių technologijų rūšių įrenginiams sunkumų gali sukelti pasikeitusi asmens išvaizda, laikas, nešvarumai ar aplinka. Biometrinės sistemos duomenų saugumas yra labai svarbus. Biometrinė sistema gali susidurti su rizika, kad duomenys gali būti pažeisti, nutekinti ar suklastoti. Dėl to jau įrašyti duomenys būna paverčiami ir saugojami šifruotų vaizdų pavidalu, kad nebūtų vizualiai suprantami žmogaus akims (Gayathri et al., 2020).

Laikui bėgant įvairios technologijos gali patirti gedimų ar sistemos trikdžių, dėl to reikia apgalvoti alternatyvas. Užtikrinant didesnį saugumą, galima naudoti 2 biometrinių rūšių autentifikavimą, kada sugedus vienai technologijai skenavimą atliktų kita. Taip pat biometrines technologijas galima naudoti su kitomis technologijomis, tokiomis kaip: RFID, kodai ar slaptažodžiai. Jeigu nutiktų taip, kad biometrinis įrenginys ar sistema sugestų, identifikavimą būtų galima atlikti arba kita biometrine rūšimi, arba kita technologija. Taip pat veikimo procese gali įsivelti klaidos galimybė, dėl to biometrinės technologijos yra vis tobulinamos, gerinamas sistemos pritaikomumas ir stengiamasi mažinti klaidų pasitaikymo galimybę.

2 lentelė. 3 pagrindinių identifikavimo būdų privalumai ir trūkumai (Faundez-Zanuy, 2006)

Identifikavimo būdai	Privalumai	Trūkumai
RFID kortelės, ID, pasas ir t. t.	• Atkartojama, galima išduoti naują • Lengvai nešiojama, galima laikyti bet kurioje vietoje	• Lengva pavogti, pamesti ar suklastoti • Gali pasinaudoti kitas asmuo
Slaptažodžiai, PIN kodai ir t. t.	• Paprasta ir ekonomiška • Galima atkurti ir pakeisti nauju	• Galima atspėti ar nulaužti • Sunku sugalvoti stiprų slaptažodį, kuris nebus pamirštas • Gali pasinaudoti kitas asmuo
Biometrinės technologijos	• Platus ir patogus panaudojimas • Negalima pamesti, pavogti, pamiršti, atspėti ir t. t. • Lengva patikrinti ir identifikuoti • Greita ir efektyvu • Mažina žmogiškojo faktoriaus klaidas • Užtikrina didesnį saugumą	• Tiksliam nuskaitymui gali turėti įtakos aplinka • Reikalauja nemažai investicijų • Laikui bėgant kinta kai kurie biometriniai duomenys

Naudojant biometrines technologijas, kuriamos duomenų bazės su biometriniais duomenimis. Svarbu skirti didelį dėmesį duomenų apsaugai ir visus duomenis apsaugoti nuo neteisėto pasisavinimo, suklastojimo ir panašiai. Dažniausiai bandoma apeiti arba jutikliui pateikti netikrą biometrinę savybę, pavyzdžiui, netikrą pirštą. Norint to išvengti, biometriniai duomenis yra tiksliai nuskaitomi ir užkoduojami, kad pašalinis žmogus negalėtų jų iššifruoti (Jain, 2005). Biometrinių duomenų apsaugai galima taikyti tradicinius šifravimo ir kriptografinius būdus, bet koks duomenų apdorojimas reikalauja iš anksto iššifruoti, todėl biometrinė informacija vis tiek tampa pažeidžiama. Šifravimo mechanizmai, specialiai sukurti biometriniam atpažinimui šablonų apsaugos pavidalu, įveikia šį pažeidžiamumą, suteikdami galimybę palyginti biometrinius duomenis šifruotoje srityje (Gomez-Barrero et al., 2022). Biometrinė sistema turi būti ne tik atspari asmenims, kurie kėsinasi įsilaužti į sistemą, pasisavinti ar nulaužti biometrinius duomenis, bet ir veikti tiksliai, greitai bei būti lengvai naudojama. Multimodalinė biometrinė sistema gali sumažinti suklastojimo galimybę, nes dvigubą identifikaciją sunkiau suklastoti.

Taigi, laikui bėgant biometrinės technologijos vis yra tobulinamos ir įgauna didesnį konkurencingumo lygį prieš kitas technologijas. Apžvelgus biometrinių technologijų sampratas, galima teigti, kad anksčiau analizuoti autoriai biometrinių technologijų sąvoką apibrėžia gana panašiai ir net vienas kitą papildo. Tai yra žmogaus identifikavimas pagal jo biometrinius duomenis. Biometrinės technologijos sukuria didesnį darbo našumą, padeda sumažinti žmogiškojo faktoriaus klaidas ir sąnaudas. Suklastoti šiuos duomenis yra beveik neįmanoma, nes kiekvienas žmogus pasižymi unikaliais biometriniais duomenimis, kurie sistemoje yra šifruojami. O norint užtikrinti didesnį saugumą, galima naudoti kelias biometrines rūšis ar kartu su kitomis technologijomis.

1.2. Biometrinių technologijų rūšys ir jų veikimo principai

Biometrinės technologijos turi daugybę skirtingų rūšių, kurios yra naudojamos asmenų tapatybės ar charakteristikų patvirtinimui. Jas galima suskirstyti pagal dvi kategorijas, fizines ir elgesio savybes turinčias biometrinių technologijų rūšis (Labayen et al., 2021) (žr. 1 pav.). Kiekvienam biometrinių technologijų rūšies skenavimui reikalingas tam tikras skenavimo įrenginys, kuris padeda identifikuoti asmenį. Kiekvienas žmogus yra unikalus ir turi skirtingus biometrinius duomenis, tačiau kiekviena biometrinių technologijų rūšis turi skirtingą saugumo lygį. Biometrinių technologijų rūšys pasižymi skirtingu pobūdžiu, panaudojimu, privalumais ir trūkumais. Didesniam saugumo užtikrinimui naudojamas kelių biometrinių technologijų rūšių autentifikavimas.

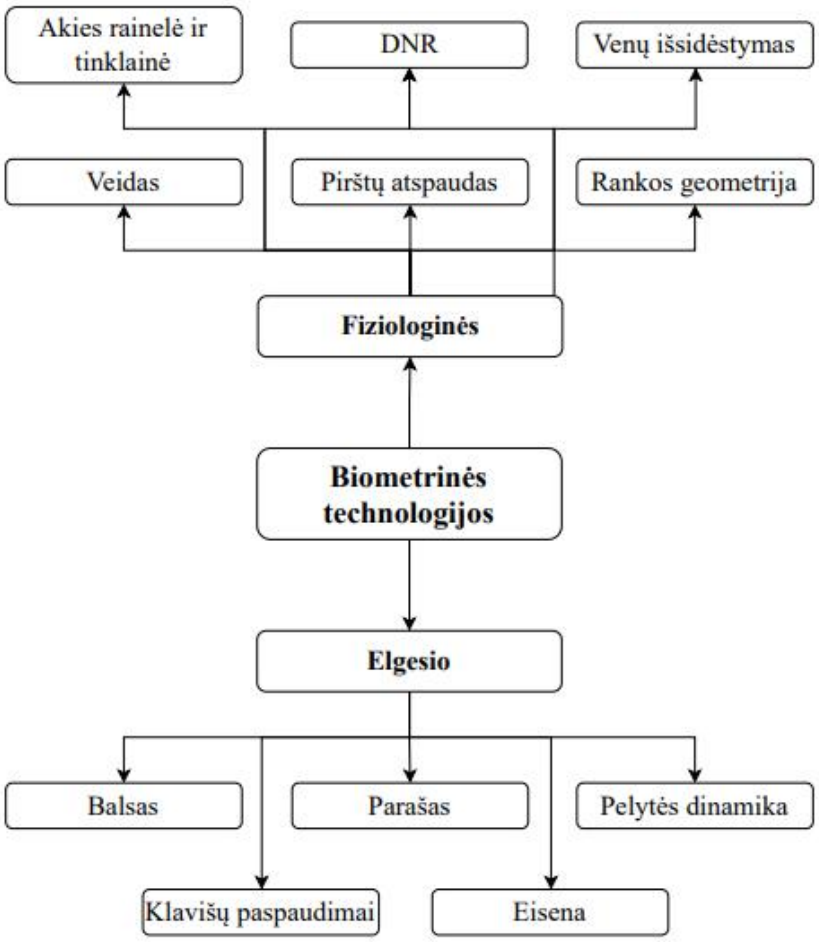
Fiziologines ypatybes turinčios biometrinės rūšys

- **Pirštų atspaudų skenavimas** – plačiausiai naudojama biometrinė rūšis, kuri užtikrina didelį efektyvumą ir tikslumą bei pasižymi mažesne kaina. Kiekvienas piršto atspaudas yra unikalus, kuris turi skirtingą piršto piešinį/atspaudą. Nuskaitymo metu piršto atspaudas yra nuskenuojamas, koduojamas ir lyginamas su jau turimais bazėje duomenimis. Pirštų atspaudai yra viena iš brandžiausių biometrinių technologijų (Jain et al., 2006).
- **Veido atpažinimo technologija** – yra taip pat plačiai išplitusi biometrinių technologijų rūšis, kuri pasižymi patogumu, kadangi nereikalauja jokio tiesioginio kontakto su prietaisu, o užtenka tapatybę nustatyti nuotoliniu būdu, tiesiog pažvelgus į vaizdo kameros objektyvą (Trukšina & Vasiliauskas, 2014). Veido skenavimo metu būna susiduriama su išvaizdos pasikeitimais, judesiu, vaizdo susiliejimu, judėjimu, dėl ko vaizdo kokybė gali būti blogesnė. Siekiant išvengti šių dalykų, šioje technologijoje reikalingas išankstinis apdorojimas, kada į sistemą galima kelis kartus pateikti veido duomenis iš visų pusių, pavyzdžiui, nusiskaityti su akiniais ir be jų (Gayathri et al., 2020). Visą tai gali užtikrinti didesnį efektyvumą ir geresnę veikimo kokybę. Šie biometriniai duomenys su laiku keičiasi, nes žmogus sensta, dėl to su laiku sistemoje reikėtų atsinaujinti biometrinius duomenis.
- **Rainelės atpažinimas** – laikoma tiksliausia ir saugiausia sistema, nes jos struktūra turi sudėtingus modelius, net identiški dvyniai pasižymi skirtingomis rainelės savybėmis. Norint gauti akies rainelės vaizdus, reikia fotoaparato su infraraudonųjų spindulių apšvietimu, kad būtų išgauta pakankamai detalių net ir tamsiai pigmentuotoms rainelėms (Gomez-Barrero et al., 2022). Rainelės nuskaitymo biometrinėje sistemoje akyje aplink vyzdį esantis spalvotas audinyspasižymi keliomis savybėmis, kad turi daug taškų, kurie yra naudojami palyginimui, įskaitant žiedus, eilutes ir dėmes (Choudhary, 2012).
- **Rankų ir pirštų geometrijos matavimas.** Nuskaitymo metu fiksuojami delno ir pirštų forma bei dydžiai, tarp jų esantys tarpai, turimi randai ir su laiku atsirandančios raukšlės. Labai svarbu kartas nuo karto atsinaujinti duomenis dėl atsirandančių raukšlių ir kintančios geometrijos. Infraraudonaisiais spinduliais jutikliai užfiksuoja venų raštus žmogaus rankos viduje (Gayathri et al., 2020).
- **Akies tinklainės skenavimas** – skenuojamas kraujagyslių išsidėstymas ir raštai. Naudojantis šiuo metodu, žmogus turi žiūrėti pro specialų objektyvą ir sutelkti žvilgsnį konkrečią regėjimo lauko vietą, ties vienu tašku. Tuo metu yra naudojamas sveikatai nekenkiantis spindulys, kuriuo atpažįsta ir išmatuoja iš anksto nustatytą. Manoma, kad šis metodas yra pats saugiausias ir

tiksliausias, nes nėra prasmės keisti ar atkartoti tinklainės kraujagyslių (Jain et al., 2006). Tinklainės tikrinimas laikomas greičiausiu apdorojimu (Gayathri et al., 2020).

Elgesio ypatybes turinčios biometrinės rūšys

- **Eisenos atpažinimas** – žmogaus indentifikavimas pagal jo ėjimo stilių yra vienas iš elgesio savybes turinčių biometrinių technologijų rūšių. Atpažinimas dažniausiai naudojamas stebėjimo programoms, kada įrenginys aptinka judantį objektą ir atlieka kūno judesių analizę pagal judesį, žingsnių dydį, greitį, žmogaus kūną, jo ir kūno dalių dydį. Ši biometrinė rūšis stebi kojų ir rankų judėjimo būdą bei ciklą (Alsaadi, 2021). Ši biometrinių technologijų rūšis turi tokį minusą, kad gali nepažinti žmogaus, kurio pasikeitė eisena dėl sulaužytos kojos, arba gali nepažinti – dėl nešamų didesnių daiktų ar vilkimų įvairaus tipo drabužių.
- **Balso atpažinimas.** Tai biometrinė atpažinimo technologija, kuri automatiškai atpažįsta kalbėtojo tapatybę pagal jo žodžių tarimo ypatybes (Yu & Li, 2018). Kaip ir kitos biometrinių technologijų rūšys balso atpažinimas pasižymi unikalumu, kadangi kiekvienas žmogus turi savo kalbėseną, skirtingas burnos ir gerklės proporcijas (Alsaadi, 2021). Balso atpažinimo sistema yra patogi, kadangi nereikalingas jos kontaktas su įrenginiu. Balso atpažinimo sistemai nereikalingi jokie brangūs įrenginiai, tai vieni iš pigesnių biometrinių duomenų skaitytuvų. Ši biometrinė rūšys atlieka balso bangų matavimą. Šis nuskaitymas atliekamas gali būti neįtint tikslus, nes susiduria su keliais minusais, tokiais kaip: emocinė būklė, užkimimas, intonacija, įrangos naudojimo ir jos būklės (Dovydaitis, 2018).
- **Parašo analizė** – biometrinė elgsenos rūšis, kuri skirta žmones identifikuoti analizuojant jų parašus internetinėje erdvėje arba tradiciškai ant popieriaus (Alsaadi, 2021). Šioje biometrinių technologijų rūšyje būna paimamas vaizdas, kuris iš anksto apdorojamas, funkcija išgaunama, pasirinktas šablonas sugeneruojamas ir saugomas duomenų bazėje (Gayathri et al., 2020). Pasirašymo metu būna analizuojamos įvairios savybės, tokios kaip: rankos judesys, greitis, rašiklio prispaudimo jėga ir kampas (Trukšina & Vasiliauskas, 2014). Naudojant parašo analizę, galima susidurti su sunkumais, kad pasirašymui įtakos turi žmogaus fizinė galia ir savijauta.
- **Klavišų paspaudimų dinamika** – žmogaus klavišo paspaudimo analizės procesas, kada žmogus identifikuojamas pagal spausdinimo ritmą. Klavišų paspaudimo metu stebima dinamika, bendras spausdinimo greičio vidurkis nuo klavišo paspaudimo iki atkėlimo (Gayathri et al., 2020). Naudojant šią biometrinių technologijų rūšį, prie sistemos nereikia prijungti išorinių techninės įrangos komponentų, užtenka turimos klaviatūros, su kuria bus renkamas tekstas (Alsaadi, 2021).



1 pav. Biometrinių technologijų rūšys (sudaryta darbo autorės)

Kaip ir kiekviena technologija, kiekviena biometrinių technologijų rūšis turi savo privalumų ir trūkumų. 3 lentelėje yra pateikiami pagrindinių biometrinių technologijų rūšių privalumai ir trūkumai. Veido atpažinimo technologija pasižymi patogumu, kai nereikia palaikyti jokio tiesioginio kontakto su prietaisu, kuris duomenis nuskaito per atstumą. Ši technologija susiduria su keliais trūkumais, kurie identifikavimo procesą paverčia ne tokį tikslų. Dėvimi aksesuarai veido srityje, pavyzdžiui, akiniai ir smarkiai pasikeitusi šukuosena gali sukelti sunkumų įrenginiui, kuris gali nebeatpažinti asmens. Laikui bėgant žmogus sensta ir veido srityje atsiranda raukšlių, kurios irgi gali turėti įtakos identifikavimui, todėl rekomenduojama kartais atnaujinti duomenų bazę. Veido atpažinimo sistemos kokybei įtaką gali daryti ir aplinka, šviesos kitimas. Šiai technologijai reikalinga kuo didesnė vaizdo raiška, kad būtų atliktas kuo tikslesnis veido atpažinimo procesas. Pirštų atspaudų skenavimo technologija pasižymi tikslumu ir patikimumu, kad atspaudus yra sudėtinga atkartoti ar suklastoti. Pirštų atspaudai laikui bėgant nesikeičia, dėl to nėra būtini duomenų atnaujinimai, tačiau jei pirštas bus sužalotas, įpjautas, tai prietaisas gali sunkiau atpažinti asmenį dėl deformuoto piršto

atspaudo. Taip pat prietaisas atspaudą gali sunkiau nuskaityti, kai pirštas ar įrenginys bus nešvarus ir infraraudonieji spinduliai per nešvarumus negalės nuskaityti atspaudo. Dar viena tiksliausia ir saugiausia yra laikoma akies rainelės nuskaitymo technologija, kuri pasižymi greitu skenavimu ir kurią sunku suklastoti. Kadangi žmogaus akies rainelė nesikeičia, dėl to nereikia atnaujinti žmogaus biometrinių duomenų, tačiau per akinius ar dideles blakstienas įrenginys gali sunkiau nuskaityti rainelę. Akies rainelės nuskaitymo įrenginys yra vienas iš brangiausių. Balso atpažinimo technologijos prietaisas daug nekainuoja. Nuskaitymo metu nėra reikalingas tiesioginis kontaktas su prietaisu, nuskaityti gali per atstumą, tačiau garso kokybei įtaką turi aplinkos garsai, žmogaus emocinė būklė, ligos ar bėgant laikui pasikeisti balso tonas. Eisenos atpažinimo prietaisas judantį objektą gali nuskaityti per atstumą. Kitas šios biometrinės rūšies privalumas yra tai, kad jai nereikia didelės raiškos vaizdo bei konkretaus jutiklio ar aparatinės įrangos. Eisenos nuskaitymo kokybei gali turėti įtakos pasikeitusi eisena dėl patirtų traumų, nešiojamu drabužių ar daiktų. Svarbu paminėti, kad visos biometrinių technologijų rūšys yra saugios, nes kiekvienas žmogus turi skirtingus biometrinius duomenis, kuriuos sunku suklastoti. Taigi pačios patogiausios ir saugiausios, kurios pasižymi daugiausiai privalumų turinčiomis biometrinių technologijų rūšimis, yra pirštų atspaudų ir akies rainelės skenavimo technologijos.

3 lentelė. Biometrinių technologijų rūšių privalumai ir trūkumai (sudaryta darbo autorės)

Biometrinių technologijų rūšys	**Privalumai**	**Trūkumai**
Veido atpažinimo technologija	• Nebūtinas kontaktas su įrenginiu	• Aksesuarai • Pasikeitusi šukuosena • Senėjimas • Aplinka • Reikalinga didelė raiška
Pirštų atspaudų skenavimas	• Patikima technologija • Sudėtinga suklastoti • Senstant nesikeičia biometriniai duomenys • Nebrangi įranga	• Nešvarumai ant piršto ar prietaiso • Būtinas tiesioginis kontaktas • Sužalotas pirštas
Rainelės atpažinimas	• Tiksliausia ir saugiausia technologija • Greitas skenavimas • Senstant nesikeičia biometriniai duomenys • Sudėtinga suklastoti	• Brangi įranga • Aplinka • Aksesuarai ant akių

3 lentelės tęsinys

Balso atpažinimas	• Nebūtinas kontaktas su įrenginiu • Nebrangi įranga	• Liga • Emocijos • Senėjimas • Aplinka
Eisenos atpažinimas	• Asmens atpažinimas per atstumą • Nebūtinas kontaktas su įrenginiu • Nereikia diegti konkretaus jutiklio ar įrenginio • Nebūtina didelė raiška	• Trauma • Daiktai • Drabužiai

Kiekviena biometrinių technologijų rūšis nuskaito skirtingus žmogaus biometrinius duomenis (žr. 4 lentelę). Skenuojant pirštų atspaudus stebimi piršto briaunų išsidėstymai, raštai, esantys tarpai tarp jų, smulkūs taškai ir poros. Net kiekvienas pirštas to paties žmogaus pasižymi skirtingu atspaudu. Taip pat ir rankos biometrijoje yra nuskaitomi raštai, įvairūs įdubimai ar raukšlės, pačios rankos ir pirštų dydis, jų perimetras ir pan. Skenuojant veidą, sistema nuskaito veido formą, burnos, akių, nosies, antakių išsidėstymą. Akies atpažinimą sudaro 2 biometrinių technologijų rūšys: rainelės ir tinklainės skenavimas. Abi rūšis infraraudonaisiais spinduliais nuskaito akies formą, blakstienas, akyje esančias dėmes, taškus ir kraujagyslių išsidėstymą. Nuskaitant balsą labai svarbu intonacija, emocinė būklė ir garso trukmė, nes šios savybės padeda identifikuoti asmenį. Identifikuojant žmogaus parašą, atsižvelgiama į laikomo rašiklio kampą, jėgą, judėjimo greitį ir sukeliamą garsą tarp rašiklio ir lapo. Klavišo paspaudimą sudaro tokios savybės kaip: asmens emocinė ir fizinė būklė, greitis bei laikas klavišo paspaudimui. Eisenos nuskaitymo metu būna fiksuojamas asmens ėjimo būdas, ciklinis judėjimas, jo greitis, ūgis bei galūnių dydžiai.

4 lentelė. Biometrinių technologijų rūšių savybės (sudaryta darbo autorės)

Biometrinių technologijų rūšis	Savybės
Pirštų atspaudų skenavimas	Briaunos, smulkūs taškai, poros
Veido skenavimas	Akys, nosis, burna, skruostikauliai, žandikauliai, raukšlės
Rainelės ir tinklainės atpažinimas	Akių vokai, blakstienos, taškai, dėmės, kraujagyslių išsidėstymas

4 lentelės tęsinys

Rankų ir pirštų geometrijos nuskaitymas	Rankos forma, delno ir pirštų dydis, įbrėžimai, raukšlės, įdubimai, kampai tarp pirštų, venos
Balso atpažinimas	Intonacija, emocinė būklė, trukmė, tonas
Parašo analizė	Judėjimo greitis, kampas, jėga, garsas
Klavišo paspaudimas	Emocinė ir fizinė būklė, greitis, trukmė klavišo paspaudimui
Eisena	Ūgis, galūnių ilgis, ėjimo būdas, ciklas, žingsnio ilgis ir greitis

Beveik visos biometrinių technologijų rūšys, nesvarbu, ar tai fiziologines ypatybes turinčios biometrinės rūšys, ar elgesio, turi pagrindinius **veikimo procesus** (Alsaadi, 2021):

1. **Registracija**. Pradinis biometrinių technologijų veikimo procesas, kuris atlieka svarbų vaidmenį biometrinių technologijų sistemoje, kadangi yra renkami žmonių biometriniai duomenys. Sukuriamas individualus šablonas kiekvienam asmeniui, kuris saugomas duomenų bazėje ir vėliau naudojamas sistemoje.
2. **Išankstinis apdorojimas**. Iš ankstesniame procese surinktų duomenų atliekamas išankstinis apdorojimas, kada yra ištrinama visa nereikalinga informacija.
3. **Duomenų išgavimas**. Labai svarbu, kad šis procesas būtų atliktas tiksliai ir efektyviai, kad būtų išgaunami kokybiški biometriniai duomenys. Gauti galutiniai duomenys konvertuojami į kompiuterinį kodavimą.
4. **Atpažinimas**. Tai pats svarbiausias ir reikšmingiausias žmogaus indentifikavimo procesas, kada aptinkamas dviejų gautų biometrinių savybių atitikimas ir yra palyginami žmogaus biometriniai duomenys su esančiais sistemoje.

Apibendrinant galima teigti, kad biometrinės technologijos turi platų rūšių pasirinkimą tarp fiziologinių ir elgesio ypatybes turinčių biometrinių technologijų rūšių, tik svarbu išsirinkti pačią tinkamiausią. Kiekviena biometrinių technologijų rūšis turi panašius veikimo principus, savus privalumus ir trūkumus. Fiziologines savybes turinčios biometrinių technologijų rūšis sudaro pirštų atspaudas, rankos geometrija, akies rainelė ir tinklainė, veidas ir DNR, o elgesio savybes turinčias biometrines technologijas – klavišų paspaudimas, eisena, parašas ir balsas. Pati populiariausia ir saugiausia biometrinių technologijų rūšis – pirštų atspaudų skenavimas. Kiekvienas žmogus turi individualius biometrinius duomenis, todėl juos suklastoti yra be galo sunku. Vis dažniau ir plačiau yra pasirenkama naudoti biometrines technologijas, kurias galima pritaikyti įvairiose srityse.

1.3. Biometrinių technologijų panaudojimo sritys ir galimybės

Biometrinės technologijos turi plačių panaudojimo galimybių įvairiose srityse, kurių pagrindinis tikslas yra nuskaityti biometrinius duomenis ir identifikuoti žmogų. Biometrinių technologijų panaudojimas pagerina teikiamų paslaugų kokybę, užtikrina didesnį saugumą ir konkurencingumo lygį. Biometrinių technologijų panaudojimas gali užkirsti kelią sukčiavimui, neteisėtam paslaugų, operacijų naudojimui ar prekių pasisavinimui. Biometrinės technologijos gali padėti patvirtinti tapatybę, pašalinti pasikartojančius ir apgaulingus dokumentus bei padėti teisėsaugos institucijoms bendradarbiauti nustatant nusikalstamą veiką (Joseph et al., 2006).

Tobulinant sąsają tarp žmogaus ir kompiuterio, yra kuriama daugybė įrenginių. Dažniausiai šie įrenginiai vis tiek naudoja žmogaus motorinius gebėjimus mechaniškai judinti tam tikras svirteles ir mygtukus (Gedminas, 2016). Buvo pastebėta, kad akių sekimo technologijose mygtuko paspaudimas fiksuojamas naudojant akies mirktelėjimus ir žiūrint į mygtuką tam tikrą laiką, kurį norima paspausti. Būtent akių sekimo sistemos leidžia tyrėjams nustatyti į ką asmuo žiūri per tam tikrą laiką ir akių judesius iš vieno taško į kitą (Albilali et al., n.d.).

Labai dažnai biometrinės technologijos yra naudojamos patekimui į pastatus, pasienio kontrolės punktus, oro ir jūros uostus, bankuose ar išmaniuosiuose įrenginiuose. Pavyzdžiui, žmonės bankomatuose, įvesdami PIN kodus, baiminasi, kad gali kažkas pamatyti skaičių kombinaciją, o šią problemą galėtų padėti išspręsti biometrinių technologijų naudojimas (Galterio et al., 2018). Kiekvienam žmogui yra suteikiamas biometrinės autentifikacijos unikalus ID, kuris yra susiejamas su asmens banko sąskaita. Taip vartotojas gali greitai ir saugiau prisijungti prie banko paskyros ar atlikti pavedimą (Muralidharan et al., 2016). Biometrinės technologijos, ypač akių nuskaitymo sistemos, naudojamos įvairiuose sektoriuose, tokiuose kaip neuromokslas, klinikiniai tyrimai, mokymasis, biomechanika, ergonomika ir rinkos tyrimai (Borgianni et al., 2018). Šiuo metu labai populiaru biometrinius duomenis naudoti išmaniosiose technologijose. Išmaniuosiuose įrenginiuose labiausiai paplitusios veido nuskaitymo ir piršto atspaudo technologijos, jos leidžia užrakinti įrenginius arba konkrečią programą. Tai užtikrina ne tik įrenginio ar programos apsaugą nuo pašalinių žmonių, bet ir leidžia savininkui greitai pasiekti informaciją be jokių slaptažodžio suvedinėjimų (Galterio et al., 2018).

Šiuo metu kai kuriose valstybėse biometrinės sistemos yra plačiai naudojamos rinkimuose, norint registruoti rinkėjus. Pavyzdžiui, Afrikoje nuolat yra susiduriama su sunkumais rengiant sąžiningus, patikimus ir skaidrius rinkimus. Technologiniai sprendimai, tokie kaip elektroniniai balsavimo aparatai, rinkimų apylinkių internetinės kameros ir biometrinė identifikavimo įranga, žada

greitas, tikslias ir apsaugotas nuo klastojimo naujoves, kurios sumažins sukčiavimą registracijos, balsavimo ar balsų skaičiavimo sumavimo procesus (Iwuoha, 2018).

Taip pat šiuo metu kelionėse reikia pateikti nemažai asmeninės informacijos, o biometrinės technologijos gali pasiūlyti aukštesnį saugumo, tikslumo ir patogumo lygį. Oro uostai nuolat stengiasi, kad kelionės būtų malonios ir patogios savo klientams. Biometrinių technologijų pritaikymas oro linijų ir oro uostų kontaktiniuose taškuose yra vienas iš tokių pramonės bandymų. Biometrinės sistemos gali užtikrinti didesnį saugumą ir efektyviau aptarnauti daugiau keleivių, nes keleivių apdorojimas yra sudėtingas. Aviacijos sektoriuje biometrinės technologijos naudojamos registruojantis oro uoste, atliekant užsakymus, įlaipinant ir ateityje atliekant bagažo išdavimo procesus (Rahman et al., 2021). Integravus biometrines technologijas į šią sritį, galima pasiūlyti daug geresnį tapatybės valdymą, žmogiškųjų išteklių valdymą ir aukštesnį patogumų lygį, naudojant tapatybės valdymo ir imigracijos sistemas, registruotų keliautojų programas, biometrinius pasus ar biometrines įėjimų į patalpas sistemas (Morosan, 2016). Oro uosto apsaugos tarnyba galės greičiau identifikuoti žmogų ir nereikės neštis bei rodyti jokio asmens dokumento pro apsaugos postą. Taip pat biometrinės technologijos gali padėti stebėti darbuotojus, jų psichinę ir fizinę būseną, tai leis stebėti, ar darbuotojai atitinka darbuotojų grupėms keliamus reikalavimus. Tokie darbo procesų stebėjimai galėtų padėti įmonėms įveikti kai kuriuos demografinių pokyčių iššūkius ir išlaikyti vyresnio amžiaus darbuotojus (Zheng et al., 2022). Skrydžių valdymo centruose, orlaiviuose ir pilotų kabinose dažniausiai yra naudojamos akių sekimo sistemos (Kaklauskas & Zavadskas, 2010).

Trukšina (2013) bei Kaklauskas ir Zavadskas (2010) išskiria tokias biometrinių technologijų panaudojimo sritis:

- rinkos tyrimams ir analizei;
- viešajame ir privačiajame sektoriuje;
- išmaniosiose technologijose;
- teisėsaugos institucijose;
- valstybinėse organizacijose, kontroliuojant įėjimą i patalpas;
- sveikatos apsaugos srityje;
- užtikrinti žmogaus saugumą;
- duomenų apsaugai;
- asmens tapatybei identifikuoti;
- žmogaus elgesio pasikeitimams analizuoti.

Kaklauskas ir Zavadskas (2010) teigia, kad taip pat biometrinės technologijos gali būti taikomos asmens sekimui. Dauguma biometrinių technologijų prietaisų identifikuoja žmones patys,

kai net to nepageidauja. Todėl kai kurios biometrinės sistemos, tokios kaip: nuotolinio veido atpažinimo,piršto atspaudų, balso įrašymo, kelia didžiausią pavojų. Kartais žmonėms gali atrodyti, kad jie yra stebimi, sekami, identifikuojami, atsižvelgiant į jų praeityje padarytus veiksmus.

Biometrinių technologijų naudojimas gali susidurti su netiksliais duomenimis dėl sugedusių ir nepakeistų detalių bei netinkamai prižiūrimų prietaisų. Ant jutiklių susikaupę nešvarumai neleis iki galo nuskaityti duomenų, dėl to gali sumažėti kokybė ir nuskaitymo tikslumas. Svarbu mokėti tinkamai naudotis prietaisais tam, kad pirminiai duomenys būtų nuskaitomi į duomenų bazę taisyklingai ir kokybiškai. Tai užtikrins, kad tolesni identifikavimo veiksmai vyktų greitai ir sklandžiai. Tam tikros biometrinių technologijų rūšys negali būti pritaikytos visiems pasaulio žmonėms, pavyzdžiui, balso nuskaitymo technologija negali pasinaudoti kurčnebyliai ar dėl nelaimingų atsitikimų ir ligų negali nuskaityti kitų biometrinių duomenų. Prieš pradedant diegti ir naudoti biometrines technologijas reikėtų įvertinti kiekvienos rūšies privalumus ir trūkumus, kad technologija atitiktų poreikius.

Yra išskiriami 7 biometrinių technologijų naudojimo reikalavimai (Jain, 2005):

- **Universalumas**. Biometrinių technologijų rūšių pritaikymo kiekvienam žmogui galimybė.
- **Išskirtinumas**. Kiekvieno žmogaus biometriniai duomenys yra skirtingi, kad būtų galima identifikuoti asmenį.
- **Patvarumas**. Dažnai nekintantys biometriniai duomenys per tam tikrą laiko tarpą.
- **Surenkamumas**. Didelis biometrinių duomenų kiekio surinkimas.
- **Našumas**. Biometrinių duomenų nuskaitymo tikslumas ir greitis.
- **Priimtinumas**. Žmonių sutikimas naudotis biometrinėmis technologijomis.
- **Apėjimas**. Rodo kaip lengvai galima apeiti sistemą neteisėtiems tikslams.

Prieš pradedant naudoti biometrines technologijas, reikėtų išsirinkti sau tinkamiausią, nes kiekviena biometrinių technologijų rūšis turi savo privalumų ir trūkumų. 5 lentelėje pateikiamos keturios pagrindinės biometrinių technologijų rūšys, jų savybės, skirtumai, gerosios ir blogosios panaudojimo pusės. Kiekvienas žmogus turi skirtingus biometrinius duomenis, dėl to juos sunku suklastoti ir saugu naudoti. Piršto atspaudo ir rainelės biometrinės sistemos yra tiksliausios ir jas padirbti yra be galo sunku. Svarbu ir tai, kad laikui bėgant šie asmens biometriniai duomenys nekinta. Veidas ir balsas turi mažesnį tikslumo lygį. Net ir naudojant biometrines technologijas, kartais gali pasitaikyti klaidų, kurias gali sukelti aplinkos veiksniai. Pirštų atspaudų naudojimas kartais gali sukelti sunkumų, nes nuskaitymui gali turėti įtakos dėvimos pirštinės, drėgmė ar nešvarumai, esantys ant pirštų ar skanerio paviršiaus. Veido nuskaitymas irgi ne visada gali būti sėkmingas, kadangi didelę

įtaką turi apšvietimas, dėvimi aksesuarai, atliktas makiažas, pakeista šukuosena ar užsiauginta barzdą. Dėl šių savybių sunkiau atpažins asmenį. Biometrinių technologijų naudojimas pasižymi ir kelias trūkumais. Senstant žmogui gali kisti kai kurios biometrinės ypatybės. Lentelėje galima matyti, kad stipriausiai gali pasikeisti veidas ir balsas, o piršto atspaudo ir akies rainelės skenavimui turi mažą įtaką. Biometrinės technologijos užtikriną aukštą saugumo lygį, piršto atspaudą ir akies rainelę yra labai sunku atkartoti ar suklastoti. Lentelėje aptartoms biometrinių technologijų rūšimis asmenys gali lengvai ir patogiai naudotis, nes biometriniai duomenys visada yra su žmogumi. Veido, rainelės ir balso nuskaitymo technologijas patogu naudoti, nes joms nereikia tiesioginio kontakto su įrenginiu, o piršto atspaudo nuskaitymo technologijai prireiks kontakto su įrenginiu. Taip pat biometrinių technologijų diegimas reikalauja nemažai investicijų, kadangi įrenginių kainos yra didelės. Iš lentelėje analizuojamų biometrinių technologijų rūšių pats brangiausias įrenginys yra akies rainelės skeneris, o balso ir veido atpažinimo įrenginiai kainuoja daug mažiau. Lentelėje vizualiai galima matyti kuri biometrinių technologijų rūšis yra saugiausia ir patikimiausia. Dažniausiai žmonės pasirenka naudoti piršto atspaudo ir akies rainelės biometrinių technologijų sistemas, nes jos yra tiksliausios, patikimiausios ir jas nesunku naudoti.

5 lentelė. Pagrindinių biometrinių technologijų rūšių tikslumas ir naudojimas (Dovydaitis, 2018)

Požymio pavadinimas	**Piršto atspaudas**	**Akies rainelė**	**Veidas**	**Balsas**
Atkartojimas	Sunkus	Sunkus	Vidutinis	Vidutinis
Paklaida	Drėgnumas, nešvarumai	Nešvarumai, prastas apšvietimas	Apšvietimas, plaukai, akiniai	Triukšmas, fiziologiniai pokyčiai, mikrofono tipas
Tikslumas	Aukštas	Labai aukštas	Vidutinis	Vidutinis
Patogumas naudoti	Geras	Vidutinis	Geras	Labai geras
Vartotojo naudojimas	Aukštas	Aukštas	Vidutinis	Mažas
Užtikrinamas saugumo lygis	Aukštas	Labai aukštas	Vidutinis	Vidutinis
Požymių kitimas bėgant laikui	Mažas	Mažas	Vidutinis	Vidutinis
Atpažinimo įrenginio kaina	Vidutinė	Didelė	Maža	Maža

Apibendrinant galima teigti, kad biometrinės technologijos yra plačiai naudojamos, dažniausiai duomenų apsaugai ir automatinio asmens autentifikavimo procedūrose, norint nustatyti konkrečius asmenis bei asmens tapatybes nustatymo procedūrose. Tuo metu sistema atpažįsta asmenį, išskirdama jį iš kitų jau saugomų biometrinių duomenų. Norint geresnių rezultatų, reikėtų išsirinkti pačią tinkamiausią biometrinių technologijų rūšį. Svarbu išmanyti šių technologijų panaudojimo galimybes ir stebėti prietaisų veikimą, nes duomenų skenavimas gali susidurti su netiksliais duomenimis dėl sugedusių bei netinkamai prižiūrimų prietaisų. Visi susikaupę nešvarumai gali turėti įtakos tiksliam duomenų nuskaitymui. Dažniausiai biometrinės technologijos yra naudojamos pastatų, kontrolės punktų perėjimui ar išmaniosiose technologijose, tačiau panaudojamo sritys vis tobulėja ir plečiasi.

1.4. Biometrinių technologijų taikymas logistikos procesuose

Kiekviena logistikos įmonė stengiasi optimizuoti ir efektyvinti logistikos procesus, tam kad visa tiekimo grandinė vyktų nuosekliai, o darbo rezultatai tik gerėtų. Technologijos padeda realiuoju laiku rinkti ir apdoroti duomenis, stebėti krovinius, transporto priemones bei darbuotojus. Modernių transporto sistemų tikslas – skatinti saugesnį ir labiau koordinuotą transporto tinklų naudojimą, teikti naujoviškas paslaugas, kurios yra susijusios su įvairiomis transporto rūšimis ir eismo valdymu (Akkaya & Kaya, 2019). Technologijos gali suteikti didesnį saugumą teikiamoms paslaugoms, klientams bei transporto vadybininkams geresnę informacijos kokybę apie jų krovinių būsenas bei jų buvimo vietą. Šių technologijų naudojimas sukuria galimybę identifikuoti logistikos procesus, darbuotojus ir jų elgesį, o tai leidžia sekti ir valdyti logistikos procesus. Kavaliauskaitė (2022) savo straipsnyje teigia, kad išmaniųjų technologijų naudojimas logistikos srityje padeda didinti efektyvumą, kontroliuoti išlaidas ir optimizuoti maršrutus bei logistikos procesus.

Grigaitė (2022) savo darbe išskiria šiuos logistikos procesus:

- klientų (vartotojų) aptarnavimas;
- transportavimas;
- atsargų valdymas;
- užsakymų tvarkymas;
- sandėliavimas;
- medžiagų valdymas;
- produkcijos pakavimas;
- informacijos apdorojimas ir tvarkymas.

Visus logistikos procesus reikia kontroliuoti, kiekvieną procesą nuolatos stebėti, nes jei vienas procesas visoje grandinėja susidurs su problemomis, tai kiti – gali strigti ar net sustoti. Biometrinių technologijų naudojimas gali padėti optimizuoti ir gerinti logistikos procesus. Shamsuzzoha & Helo (2011) išskiria šiuos biometrinių technologijų taikymo tikslus logistikos srityje:

- konkurencinis pranašumas;
- atitiktų klientų poreikius;
- stiprinti savo pozicijas rinkoje;
- paprastinti ir pagerinti surinkimo bei pristatymo procesus;
- gražinamų užsakymo kiekių mažinimas;
- mažinti žmogiškojo faktoriaus klaidas.

Logistikoje biometrinės technologijos gali dar turėti ir šiuos taikymo tikslus:

- krovinio stebėjimas ir sekimas;
- stebėti krovinio kokybę;
- sumažinti logistikos sąnaudas;
- bendradarbiauti, sudarant sąlygas verslo partneriams dirbti kartu.

Gamybos įmonėms yra svarbu siuntų sekimas, atsižvelgiant į klientų aptarnavimą ir efektyvų logistikos tinklų valdymą. Siuntos sekimas leidžia stebėti jos buvimo vietą nuo to momento, kai kurjeris paima siuntą iki pristatymo galutiniam gavėjui. Pati sistema gali nustatyti krovinio buvimo vietą ir informuoti klientą. Norint pristatyti didėjančius produktų srautus per trumpesnį laiką, verčia įmones naudoti moderniausias technologijas. Tai padeda padidinti pelną ir įgyti gyvybiškai svarbų konkurencinį pranašumą prieš kitas panašias paslaugas teikiančias įmones. Stebėjimo ir sekimo technologijos apima brūkšninį kodą, RFID, magnetinę juostelę, optinį simbolių atpažinimą, balso ir vaizdo sistemas (Shamsuzzoha & Helo, 2011). Į krovinio stebėjimo sistemas, norint labiau apsaugoti krovinį, dažniausiai integruojamos rainelės nuskaitymas, rankos ir piršto atspaudo atpažinimo biometrinės technologijos. Kroviniai, kuriuos norima sekti, turi turėti jutiklius, kurie turi įmontuotus biometrinių duomenų skaitytuvus. Jie yra skirti rinkti informacijai ir juos perduoti į centralizuotą sistemą. Tai patogu naudoti, nes renkant duomenis iš judančių objektų, nereikia jokių laidų, visa informacija surenkama ir perduodama savarankiškai per atstumą (Jandl et al., 2021).

Biometrinės technologijos gali palengvinti, automatizuoti šalių sienų patikrinimus ir užtikrinti greitesnį, sklandesnį ir efektyvesnį darbą. Dažniausiai žmonių kontrolę atlieka apmokyti pareigūnai, kurie lygina pasą su fizine žmogaus išvaizda, o kai kur tai atlieka automatizuotos sienų kontrolės sistemos (Thenuwara et al., 2022). Su biometrinėmis technologijomis žmonės, kirsdami

sienas, galės patogiau ir veiksmingiau pereiti patikrinimus, o pasieniečiai lengviau atpažins apsimetėlius. Taip pat biometrinės technologijos padėtų išvengti šališkumo, klaidų galimybės ir neteisėtų dokumentų klastojimų ar kito asmens dokumento pasisavinimo (Galterio et al., 2018). Pastaruoju metu pasaulis bando diegti įvairias galimybes biometrinių technologijų naudojimui, kad padėtų gausėjantiems kertančių žmonių kiekiams ir ribotiems sienų kontrolės ištekliams. Dažnai biometrinės technologijos yra naudojamos kartu su asmens dokumentų tikrinimais. Tai pagerina apsaugą ir stiprina Europos Sąjungos išorines sienas (Abomhara et al., 2021). O jeigu sutrumpės pasienio patikros laikas, tai kelių transportas galės sutaupyti daugiau laiko ir greičiau pristatyti krovinius galutiniam gavėjui.

Labai svarbu apsaugoti krovinius nuo vagysčių, apiplėšimų ir neteisėto jų perdavimo. Pagerinti patalpoje esančių objektų apsaugą gali biometrinių technologijų integravimas į sandėlio sistemas. Prieigai prie pastatų ar įrangos naudojami slaptažodžiai, asmens identifikavimo numeriai, žetonai, raktai, kodai, identifikavimo kortelės ir pan. Tačiau šie metodai turi svarbiųtrūkumų – jie gali būti pamesti, pavogti, suklastoti arba pamiršti. Biometrinės technologijos gali suteikti daugiau saugumo, kontroliuojant darbuotojus, prieigą prie pastatų ir įrangos, kai technologijos atpažįsta asmenis pagal jų biologines ar elgesio ypatybes, pavyzdžiui, pirštų atspaudus, rainelės modelius, veido savybes ir kalbos modelius (Lawton, 1998). Pirštų atspaudų ir akies rainelės biometriniai duomenys yra saugūs ir tikslūs, kadangi kiekvienas žmogus turi skirtingus biometrinius duomenis, o laikui bėgant jie nesikeičia. Biometrinė apsaugos sistema naudoja vieną ar daugiau jutiklių, pavyzdžiui, kamerą ar mikrofoną, ir perduoda duomenis į skaitmeninį signalų procesorių analizei, skaitmeninimui ir apdorojimui. Pačiame sandėlyje įrengtą biometrinį autentifikavimą galima papildyti su slaptažodžio identifikavimo sistemomis.Taikant šį metodą, vartotojas įveda slaptą frazę, pateikia ją biometrinei autentifikavimo sistemai, kad patvirtintų identifikatoriaus tapatybę (Panischev et al., 2020).

Įdiegus biometrines technologijas transporto priemonėse, daug dėmesio skiriama įvairiems segmentams, įskaitant pačios transporto priemonės užvedimo jungiklį, transporto priemonės imobilizatorių, racionalizavimą ir sveikatos stebėjimą (*Adoption of Biometrics in the Automotive Industry*, 2017). Vilkikų vairuotojai susiduria su sąlygomis, kurios skatina svorio augimą. Sėdimas darbas, netinkama mityba padidina nutukimo, diabeto, lėtinių ligų ir bendro mirtingumo riziką. Nutukimas taip pat yra susijęs su miego problemomis, jos padidina avarijų riziką (Olson et al., 2016). Darbas pamainomis, kintantys grafikai ir nepalankios miego sąlygos kelia vairuotojams miego problemų riziką. Vilkikų vairuotojų darbo kokybei turi įtakos ir jų būsena ir stresas. Tokį psichologinį poveikį galima nustatyti išmatuojant ir analizuojant širdies nervus. Širdies ritmo kintamumo analizė

puikiai tinka norint įvertinti stresą ir įtampą, kai yra mažas kūno judėjimo triukšmas (YUDA et al., 2021).

Biometrinius žmogaus duomenis padeda stebėti ir atpažinti įmontuoti išmanūs jutikliai ir priedai, tokie kaip giroskopas, jutiklinis ekranas, akselerometras, orientacijos jutiklis ar slėgio jutiklis (Baldini et al., 2019). Pirštų atspaudų ir akies rainelės nuskaitymo technologijos yra laikomos pačios tiksliausios ir saugiausios, todėl rekomenduojama būtent jas diegti į transporto priemones. Transporto priemonėje biometrinės technologijos gali būti įdiegtos kaip sistemos dalis, kuri jau yra integruota transporto priemonėje. Pavyzdžiui, biometrinė sistema galėtų būti įdiegta ant transporto priemonės durų arba prie variklio uždegimo sistemos. Su variklio užvedimo raktu galėtų būti naudojamas vairuotojo piršto atspaudo autentifikavimas. Dažniausiai rainelės atpažinimo technologijos diegiamos galinio vaizdo veidrodėliuose ir gali būti pritaikytos skirtingos automobilio funkcijos skirtingiems vairuotojams (Ćatović & Adamović, 2017).

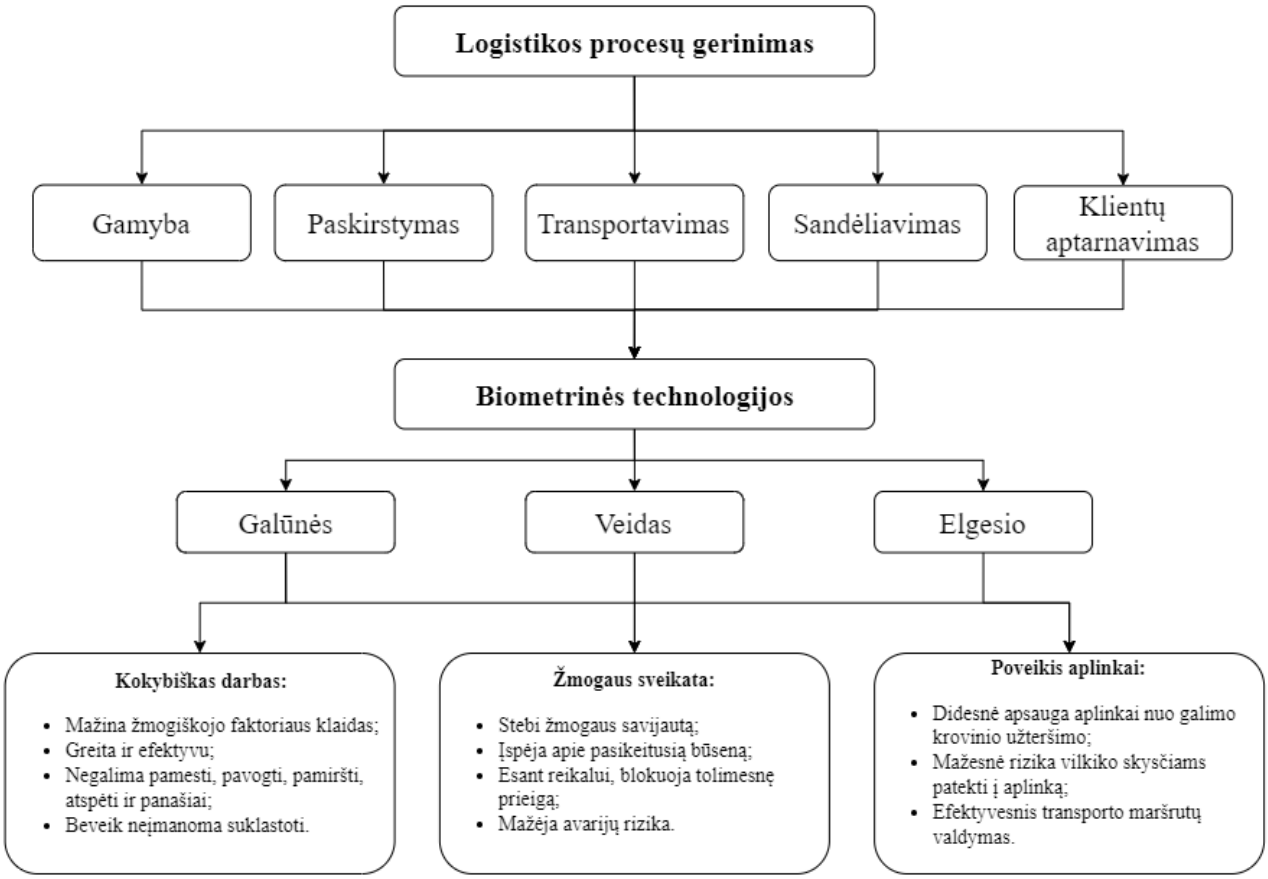
Taip pat vilkiko viduje gali būti įrengta kamera su biometrine sistema, kuri stebi vairuotoją, jo būseną ir sveikatą. Rainelės atpažinimo sistema gali stebėti, ar vairuotojo akys nėra mieguistos, ar jis nesiblaško, tokiu atveju transporto priemonė įspėja vairuotojus. Biometrinė sistema vairuotojui leidžia pagal savo biometrinius duomenis pritaikyti transporto priemonės funkcijas, pavyzdžiui, sėdynės ir veidrodėlių padėtis, muzikos stilių, temperatūrą ir panašius parametrus. Naudojant biometrines technologijas, galima įvesti kelių asmenų biometrinius duomenis, kurie naudosis ta transporto priemone. Įdiegus transporto priemonėje balso atpažinimo technologiją, įrangą gali atpažinti žmogų pagal jo balso savybes. Vairuotojas gali sugalvoti savo frazę ar numerį, kurį tardamas galės prisijungti prie biometrinės sistemos (Villemure et al., 2018). Žmonių, kurie norės pasinaudoti transporto priemone, biometriniai duomenys bus lyginami su duomenų bazėje esančiais duomenimis ir esant reikalui blokuotų prieigą (Rivandi et al., 2019). Naudojant dvigubą identifikaciją, transporto priemonė yra dar labiau apsaugota nuo vagysčių.

Apibendrinant galima teigti, kad biometrinės technologijos gali padėti gerinti ir optimizuoti logistikos procesus. Naudojamos biometrinės technologijos sukuria didesnį pranašumą prieš konkurentus, kadangi jos suteikia galimybę pagreitinti ir palengvinti valstybių sienų kirtimus, suteikia prieigą prie pastatų ir naudojamos įrangos. Taip pat padeda stebėti vairuotoją ir gabenamą krovinį, jų būklę. Tai pagerina teikiamų paslaugų kokybę. Automatizuota transporto priemonių apsaugos sistema yra svarbi šiuolaikinių automobilių technologijų galimybė norint pagerinti saugumo lygį. Transporto priemonėje galima pritaikyti pirštų, rankų atspaudų nuskaitymo, veido, balso ar rainelės nuskaitymo biometrines sistemas, jos veikia tiksliai ir patikimai. Naudojant pirštų atspaudus ar rainelės

nuskaitymus, vartotojas į sistemą gali įsivesti ilgalaikius duomenis, kadangi šių biometrinių sistemų duomenys žmoguje beveik nesikeičia.

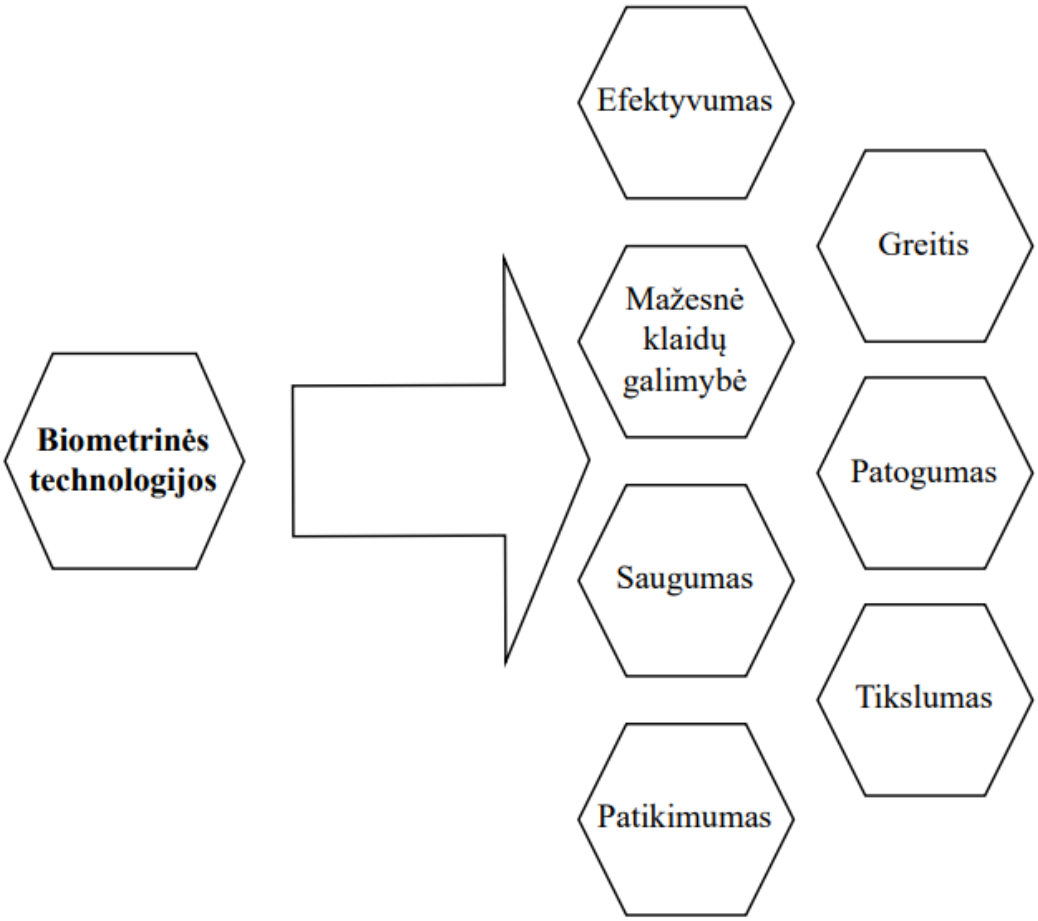
1.5. Teorinės analizės apibendrinimas

Apibendrinant pirmąjį skyrių, remiantis užsienio ir Lietuvos autoriais, galima teigti, kad biometrinės technologijos turi didelį pranašumą prieš kitas naudojamas technologijas, nes biometrinių duomenų negalima pamiršti, pamesti ir sunku suklastoti. Pagal mokslinės literatūros analizę, buvo sudarytas pirminis teorinis modelis (žr. 2 pav.). Biometrinės technologijos turi didesnį pranašumą prieš kitas technologijas, kadangi asmens biometriniai duomenys yra unikalūs, kurių beveik neįmanoma suklastoti. Biometrinės technologijos, priešingai nei kitos technologijos, gali stebėti žmonių būklę ir įspėti apie jo būsenos pakitimus.



2 pav. Teorinis modelis (sudaryta darbo autorės)

Šifruoti biometriniai asmens duomenys gali būti laikomi duomenų bazėje arba decentralizuotame įrenginyje. Prieš pradedant naudoti šias technologijas, reikėtų pasirinkti tinkamiausią rūšį. Jos skirstomos į fiziologines ir elgesio ypatybes turinčius biometrinius duomenis. Fiziologinės ypatybės yra patikimesnės, nes jos gali užtikrinti didesnį saugumą ir veiksmingesnį biometrinių technologijų veikimą, o elgsenos – ne visada gali būti tikslūs, kadangi jiems įtakos turi emocinė būklė, patiriamas stresas ar liga. Kiekviena biometrinių technologijų rūšis yra skirtinga ir turi savų privalumų bei trūkumų. Norint užtikrinti dar didesnį saugumą, galima naudoti kelias biometrinių technologijų rūšis arba kartu su kitomis technologijomis.



3 pav. Biometrinių technologijų poveikis (sudaryta darbo autorės)

3 paveiksle yra pateikiamas biometrinių technologijų poveikis. Biometrinės technologijos gali užtikrinti didesnį saugumą, patikimumą, tikslumą ir sumažinti žmogiškojo faktoriaus klaidas. Kiekvieno žmogaus biometriniai duomenys yra unikalūs, pasižymi skirtingais taškų ir briaunų išdėstymais, dėl to juos labai sunku suklastoti ar neteisėtai pasisavinti. Biometrinis duomenų

skenavimas vyksta greitai ir tiksliai, nes žmogus biometrinių duomenų nepames ir daugumai biometrinių technologijų rūšių nereikia tiesioginio kontakto su prietaisu. Kai kurios biometrinių technologijų rūšys gali pasižymėti duomenų kitimu ir sukelti sunkumų nuskaitymo metu, nes bėgant laikui žmogus sensta. Pačios saugiausios ir patikimiausios biometrinės technologijos – akies rainelės skenavimas ir pirštų atspaudų skenavimas, nes jas sunkiausia suklastoti ir ilgainiui duomenis nesikeičia. Biometrinės technologijos dažniausiai naudojamos automatiniam asmens identifikavimui ir autentifikavimui. Biometrinės technologijos yra plačiai naudojamos: viešajame ir privačiajame sektoriuje, išmaniosiose technologijose, įėjimo ar transporto priemonės kontrolei ir t. t. Tai leidžia užtikrinti teikiamų paslaugų efektyvumą ir didesnį konkurencinį lygį.

2. LOGISTIKOS PROCESŲ TOBULINIMO PANAUDOJANT BIOMETRINES TECHNOLOGIJAS TYRIMO METODIKA

2.1. Empirinio tyrimo metodologija

Išanalizavus mokslinę literatūrą, galima teigti, kad biometrinės technologijos gali palengvinti darbus, sumažinti klaidų galimybes ir užtikrinti didesnį saugumą. Norint plačiau išanalizuoti biometrinių technologijų panaudojimą logistikos srityje, buvo atliktas empirinis tyrimas.

Empirinio tyrimo tikslas – ištirti ir įvertinti biometrinių technologijų panaudojimo logistikos srityje galimybes bei pateikti siūlymus biometrinės transporto sistemos modeliui sudaryti.

Tyrimo problema – Ar įmanoma pagerinti tiekimo grandinės procesų saugumo lygį panaudojant biometrines technologijas?

Tyrimo objektas – biometrinės technologijos logistikoje.

Hipotezė – biometrinės technologijos didina saugumo lygį ir padeda išlaikyti sėkmingai veikiančius tiekimo grandinės procesus.

Empirinio tyrimo tikslui pasiekti keliami šie tyrimo uždaviniai:

1. Taikant kiekybinį tyrimo metodą, išsiaiškinti biometrinių technologijų panaudojimo logistikos srityje tyrimo dalyvių nuomonę.
2. Taikant kokybinį tyrimo metodą, išanalizuoti atrinktų biometrinių technologijų komponentų svarbą logistikos srityje.
3. Apibendrinus empirinio tyrimo rezultatus, pateikti biometrinių technologijų panaudojimo modelį logistikoje bei įvertinti logistikos ekspertų požiūrį į siūlomą modelį.

Empirinis tyrimas – įvairių būdų informacijos surinkimas, kontaktuojant tyrėjui ir tiriamajam objektui (Kardelis, 2022). Vienas iš empirinių tyrimų yra kiekybinis tyrimo metodas.

Kiekybinis tyrimo metodas – struktūrizuotas empirinis tyrimas, kurio rezultatus galima pateikti skaičiais (Gutauskaitė, 2009). Kiekybinis tyrimas pasižymi duomenų gausumu ir objektyvumu. Kiekybiniams tyrimams būdinga, kai pirmiau yra formuluojama problema ar hipotezė, išanalizuojama literatūra, o vėliau renkami duomenys, kurie yra lyginami su faktais. Taip yra dėl to, kad surinkti duomenys gali turėti įtakos problemai ir dėl to gali reikėti rinkti daugiau duomenų. Kiekybinių duomenų rinkimo metodai gali būti: apklausa, statistinių duomenų analizė, eksperimentas. Pats populiariausias ir dažniausiai naudojamas yra apklausos metodas. Remiantis moksliniais metodais yra sudaroma imtis. Tyrėjas kontroliuoja visą įvykių eigą bei laikosi numatyto plano. Taip pat tyrėjas respondentams pateikia iš anksto paruoštus ir struktūrizuotus klausimus, o

gautus rezultatus – susistemina į bendrą duomenų analizę (Bilevičienė & Jonušauskas, 2011). Apklausoje klausimai turi būti pateikti trumpi ir aiškūs, kad respondentai galėtų lengvai suprasti klausimo prasmę ir neskatintų pasirinkimo į tam tikrą klausimą. Apklausa pasižymi tam tikra struktūra, joje gali būti pateikiami tiek atviri, tiek uždari klausimai (Kardelis, 2022).

Kokybinis tyrimo metodas – nestruktūrizuotas empirinis tyrimas, kai analizuojama pasirinktų žmonių ar grupių patirtys ir įvykiai. Šio tyrimo tikslas suprasti tiriamojo elgesį, savijautą ir kokį poveikį jam turi aplinkos veiksniai (Gutauskaitė, 2009). Kokybinis tyrimas dar gali būti vadinamas interpretaciniu tyrimu, kurio metu yra remiamasi respondento elgesio pakitimais ir pažinimu. Gali būti tokie kokybiniai tyrimo metodai: interviu, atvejo analizė, stebėjimas ar diskusija. Kokybiniai tyrimai yra atliekami su mažesniu respondentų kiekiu. Kokybiniam tyrimui respondentai yra tikslingai atrenkami pagal tikslinę grupę (Kačerauskas, 2014). Kokybinis interviu yra sudarytas iš atvirų klausimų, į kuriuos tyrėjas tikisi, kad bus atsakyta kuo plačiau ir išsamiau. Šis tyrimas yra lankstus, neturi standartinės tyrimo struktūros, nepriklauso nuo iškeltų hipotezių ir visa įvykių eiga yra nekontroliuojama tyrėjo. Interviu metu vyksta pokalbis tarp tyrėjo ir respondento ar tikslinės dalyvių grupės, kai pokalbis vyksta natūraliai, nėra iš anksto apibrėžtų ribų ir respondentui nėra pateiktų atsakymų variantų (Gaižauskaitė & Valavičienė, 2016).

Duomenys – visų empirinių tyrimų pagrindas (Kardelis, 2022). Duomenys, kurie tinkamai surenkami, yra patikimi, dėl kurių gauti tyrimo išvados ir rezultatai yra tikslūs bei pagrįsti. Taip pat Kardelis (2022) teigia, kad kiekybinis ir kokybinis tyrimo metodas vienas kitą papildo. Kiekybinis tyrimas siūlomas naudoti atradimams, o kokybinis – jau atrastiems dėsniams ir teorijoms patvirtinti. Sudarant tyrimams klausimus labai svarbu juos parinkti tinkamus, nes nuo to priklausys tyrimo efektyvumas.

2.2. Tyrimo metodai ir eiga

Empiriniam tyrimui atlikti buvo pasirinkti šie tyrimo metodai:

- **Anketinės apklausos metodas**. Anketinei apklausai atlikti pasirinkti respondentai, dirbantys logistikos srityje. Šiame tyrime respondentams buvo pateikti uždarieji ir atvirieji klausimai elektroniniais laiškais ar žinutėmis per socialinius tinklus, kuriais tyrėjas siekė surinkti iškeltos tyrimo problemos informaciją ir vėliau palyginti duomenis tarpusavyje. Labai svarbu, kad klausimai būtų pateikti trumpai ir aiškiai, kad respondentas galėtų juos lengvai suprasti bei nesukeltų dviprasmybių. Tiksliau suformuluoti klausimai ir galimi atsakymai leidžia kokybiškiau apibendrinti gautus rezultatus. Visi tyrimo dalyviai galėjo į apklausos klausimus atsakyti anonimiškai, neatskleidžiant savo asmeninių duomenų.

- **Pusiau struktūrizuotas ekspertinis interviu**. Šiam metodui yra būdinga vidinė struktūra, kai iš anksto paruošiami galimi klausimai, kurie yra susiję su tyrimo tema. Pokalbis gali vystytis ne pagal planą, respondentai gali laisvai dėstyti savo mintis. Tyrėjas pokalbio metu neturi reikšti savo nuomonės klausimų tematika ir daryti įtakos respondentų atsakymams (Bilevičienė & Jonušauskas, 2011). Šiame tyrime respondentai buvo pasirinkti pagal tikslinės grupės savybes. Pagrindinis kriterijus – kompetencija. Buvo atrinkti logistikos ekspertai, dirbantys ir užimantys vadovaujamas pareigas logistikos srityje bei yra įgiję aukštąjį išsilavinimą.

Tyrimo eiga. Kiekybinio ir kokybinio tyrimo metodai atlikti 2023 metų gegužės ir spalio mėnesiais, per kuriuos pavyko surinkti reikiamų respondentų skaičiaus atsakymų rezultatus.

Anketinė apklausa buvo atliekama *apklausa.lt* interneto puslapyje, kurio internetinė nuoroda buvo siunčiama nustatytos tikslinės grupės asmenims elektroniniu paštu arba per kitas naudojamas programas. Respondentų kontaktų buvo ieškoma per krovinių biržą *cargo.lt*. Pusiau struktūrizuotas ekspertinis interviu vyko susisiekiant elektroniniu paštu arba per socialinius tinklus, prieš tai pasiruošiant galimus klausimus. Apklausimo būdas buvo pasirenkamas pagal eksperto norus ir poreikius. Logistikos srities ekspertų kontaktų buvo ieškoma krovinių biržoje *cargo.lt,* interneto puslapyje *rekvizitai.lt* ir „LinkedIn“ socialiniame tinkle. Surinkus reikiamus tyrimų atsakymų skaičius, pateikti tyrimų rezultatai. Kiekybinio ir kokybinio tyrimo klausimai yra pateikti darbo prieduose.

2.3. Tyrimo duomenų rinkimo organizavimas ir imtis

Tyrimui atlikti buvo taikomi du anksčiau darbe aptarti metodai: kiekybinis ir kokybinis tyrimas. Kiekybiniam tyrimui atlikti buvo pasirinktas anketinės apklausos metodas, kuriame pateikiami tiek uždarojo, tiek atvirojo tipo klausimai. O kokybiniam tyrimui pasirinktas pusiau struktūrizuotas ekspertinio interviu tyrimas, kuriame ekspertai buvo apklausti elektroniniu paštu arba per socialinius tinklus.

Anketinė apklausa. Rengiant anketinės apklausos klausimyną buvo remiamasi atliktos teorinės analizės duomenimis. Kaip jau minėta anksčiau, apklausoje buvo pateikti tiek atviri, tiek uždari klausimai. Atviruosiuose klausimuose nėra pateikiami galimi atsakymai ir respondentui reikėjo pačiam įvesti savo atsakymą. Apklaustieji atsakydami į šiuos klausimus galėjo laisvai reikšti savo mintis ir dalintis idėjomis. Uždaruosiuose klausimuose pateikti galimi atsakymai, kurie leido lengviau juos išreikšti skaičių pavidalu, lengviau grupuoti ir lyginti su kitų naudojamų tyrimų rezultatais. Sudarant anketinę apklausą, reikia atkreipti dėmesį į klausimus ir atsakymus, kad jie būtų gerai suprantami, parašyti be klaidų, nebūtų per daug abstraktūs, neįžeistų ir nepastūmėtų respondento

rinktis tam tikro atsakymo. Taip pat klausimai neturėtų būti monotoniški ir klausimų skaičius neturėtų varginti respondento (Tidikis, 2003). Anketinė apklausa buvo atliekama anonimiškai, todėl nebuvo surinkti jokie individualūs duomenys. Negalima identifikuoti asmenų ir matyti jų atsakymų, kurie atsakė į klausimus. Apklausą sudarė 19 klausimų, kuriais buvo siekiama išsiaiškinti respondentų biometrinių technologijų bei jų panaudojimo galimybių nuomonę ir įžvalgas.

Anketinės apklausos patikimumas. Apklausoje klausimai turi būti tikslūs ir atitikti realybę. Taip anketos rezultatai bus patikimesni ir tiksliau atvaizduos tikrovę. Kiekvieną anketą reikėtų patikrinti iš praktinės pusės: ar klausimai yra tinkamai suformuluoti ir suprantami, ar visi klausimai yra tinkamos tematikos, ar yra nuoseklumas ir išsamumas. Sudarius anketinės apklausos klausimyną, reikėtų jį atlikti su mažesne 25–30 žmonių grupe. Tai leis nustatyti klausimyno privalumus ir trūkumus (Tidikis, 2003). Tuo vadovaujantis prieš pateikiant apklausą nustatytai tiriamųjų grupei, buvo pasidalinta apklausa tik 1 logistikos įmonėje. Įvertinus klausimų, atsakymų kokybę bei tikslumą, apklausa buvo pasidalinta ir su kitomis įmonėmis.

Kiekybinio tyrimo imtis. Prieš atliekant tyrimą, reikia nustatyti tyrimo imtį. Generalinė aibė – tai visuma, kurią galima ištirti. Dažniausiai dominančių požymių paskirstymas nežinomas generalinėje aibėje, o norint tą nustatyti, reikia ištirti visus generalinės aibės elementus, o tai gali pareikalauti nemažai laiko ir pinigų, o kartais toks tyrimas gali būti neįmanomas (Kardelis, 2022). 6 lentelėje yra pateikiamos reikšmės imties dydžiui nustatyti su 5 % imties paklaida.

6 lentelė. Reikšmės imties dydžiui nustatyti (su 5 % paklaida) (Galatiltytė, 2022)

Generalinės visumos dydis	500	1000	2000	3000	4000	5000	10 000	100 000
Imties dydis	222	286	333	350	360	370	385	398

Socialinių mokslų darbuose dažniausiai yra pasirenkamas 95 % patikimumas ir imties paklaida – 5 % (Kardelis, 2022). Anketinės apklausos imtis apskaičiuota panaudojant Paniotto formulę. Ši formulė padeda apskaičiuoti tinkamą imties dydį, kad būtų galima padaryti išvadas apie visą populiaciją su tam tikru patikimumu ir paklaidos lygiu:

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

Čia: 1)

n – imties dydis;

Δ – imties paklaidos dydis;

N – generalinės visumos dydis.

Siekiant įvertinti tyrimo kokybę, iš Oficialiosios statistikos portalo (Darbo rinka Lietuvoje (2022 m. leidimas)) buvo paimtas vidutinis darbuotojų skaičius 2021 m. transporto ir saugojimo srityje. Tyrimo metu analizuojamos generalinės aibės visuma – 147 379 tūkstančiai darbuotojų logistikos srityje.

Paklaidos dydis pasirinktas, kai patikimumas 95 % ir imties paklaida 5 %:

$$n = \frac{1}{0{,}05^2 + \frac{1}{147\,379}} = \frac{1}{0{,}0025 + 0{,}0000067852} = \frac{1}{0{,}00250679} \approx 399$$

(2)

Atlikus skaičiavimus pagal Paniotto formulę, galima matyti, kad anketinės apklausos tyrimo imtis yra 399 respondentai. Pasitelkiant šį tyrimo metodą, pavyko surinkti 400 respondentų atsakymus.

Pusiau struktūrizuotas ekspertinis interviu. Sudarant ekspertinio interviu klausimus buvo atsižvelgiama į tyrimo problematiką. Galimi ir būtini klausimai buvo paruošti iš anksto. Pusiau struktūrizuotas ekspertinis interviu yra lankstaus pobūdžio, kai pokalbiui nėra numatomas joks tikslus planas, o nuo gautų atsakymų gali išsirutuliuoti papildomi klausimai (Tidikis, 2003). Interviu buvo stengiamasi kuo daugiau sužinoti apie tyrimo objektą. Respondentams buvo pateikta lentelė ir 9 atviri klausimai, kur laisvai galėjo reikšti savo mintis. Svarbu tyrėjui nenukreipti pašnekovo atsakymo tam tikra linkme.

Ekspertiniam tyrimui atlikti rangavimo būdu pasirinktas DEMATEL metodas. DEMATEL (angl. *Decision Making Experiment and Evaluation Laboratory Method*) – vienas iš MCDM (angl. *Multi-criteria decision making*) sprendimų priėmimo metodų (Koca & Yıldırım, 2021). DEMATEL metodas padeda nustatyti ryšius tarp komponentų ir išskiria pagrindinį komponentą, kuris yra pats veiksmingiausias. Šis modelis naudojamas kompleksiniams problemų sprendimams ir vertinimui, kai

yra daug alternatyvų ir kriterijų (Vinogradova, 2015). DEMATEL yra veiksminga priemonė nustatyti priežasties ir pasekmės ryšius, kurie sieja nagrinėjamą objektą (Dytczak & Ginda, 2016).

Rangavimui buvo pateikta matrica lentelės pavidalu su 9 komponentais. Komponentai, kuriuos respondentai išskyrė anketinės apklausos metu:

1. **Konkurencingumas (C1).**
2. **Prieigos kontrolė (C2).** Šis punktas gali apimti patekimą į patalpas, prieigą prie išmaniųjų technologijų ar net prieigą prie transporto priemonių.
3. **Intelektinės transporto sistemos (C3).** Išmaniosios sistemos yra šiuolaikinio pasaulio dalis, be kurių jau retas įsivaizduoja savo darbą ir kasdienybę. Technologijos nuolatos yra tobulinamos ir pritaikomos greitesniam bei lengvesniam darbo atlikimui.
4. **Saugumas (C4)**. Įmonės susiduria su dideliu informacijos kiekiu, kurį turi išsisaugoti tik įmonės viduje. Logistikos įmonėms yra be galo svarbu pristatyti krovinį galutiniam gavėjui tvarkingą ir nepažeistą.
5. **Darbuotojo ir transporto priemonės stebėjimas realiuoju laiku (C5)**.
6. **Darbuotojo sveikatos stebėjimas (C6)**.
7. **Technologijų patikimumas (C7)**.
8. **Mažesnė žmogiškųjų klaidų galimybė (C8)**.
9. **Mažesnė įsilaužimų ir vagysčių atvejų tikimybė (C9).**

DEMATEL metodo atlikimo etapai

1 etapas. Norint išanalizuoti priežastinius ryšius tarp komponentų, reikalingas ryšio įvertinimas balais. Komponentų tiesioginės įtakos intensyvumui įvertinti naudota penkių laipsnių tiesioginės įtakos skalė 0–4. (žr. 7 lentelę).

7 lentelė. Priežastinių ryšių vertinimo balai (sudaryta darbo autorės)

Balas	Reikšmė
0	Nėra ryšio
1	Labai silpnas ryšys
2	Silpnas ryšys
3	Stiprus ryšys
4	Labai stiprus ryšys

2 etapas. Kadangi tyrime dalyvauja daugiau nei vienas ekspertas, matrica X turi būti sudaroma iš balų aritmetinio vidurkio. Visų ekspertų balų aritmetinis vidurkis buvo sudaromas pagal šią formulę:

$$Z = \frac{a_1 + a_2 + \ldots + a_n}{n}$$

Čia: 3)

Z – balų aritmetinis vidurkis;

a_1, a_2, ..., a_n – balai, kurių vidurkis skaičiuojamas;

n – komponentų skaičius.

3 etapas. Tiesioginio ryšio matricai $0 \leq X_{ij} \leq 1$ sudaryti yra pasitelkiama ši formulė:

$$X = \frac{Z}{S}, \text{ kur } S = \max_{1 \leq i \leq n} \sum_{j=1}^{n} Z_{ij}$$

Čia: 4)

Z – balų aritmetinis vidurkis;

S – balų sumos didžiausia reikšmė;

n – balai.

4 etapas. Apskaičiuojama bendra matrica T.

$$T = X(I - X)^{-1}$$

5)

5 etapas. Toliau apskaičiuojamos vektorių R ir C reikšmės, susumavus atitinkamai matricos eilutes ir stulpelius. Iš susumuotų eilučių ir stulpelių gaunamos R+C ir R-C reikšmės.

$$R = \left[\sum_{j=1}^{n} t_{ij}\right]_{nx1}$$

6)

$$C = \left[\sum_{i=1}^{n} t_{ij}\right]_{1xn}^{T}$$

7)

Kokybinio tyrimo imtis. Kaip jau minėta anksčiau, kokybinio tyrimo dalyviai buvo atrinkti pagal kriterijus, kuriems būtų aktuali tyrimo problema, nes vertinimo srities ekspertai turi daugiau žinių ir patirties. Interviu tikslas – įvertinti tam tikrais požiūriais asmenį, išrinkti tikslinės grupės darbuotoją, kuris padės rinkti informaciją tyrimams ir plėtoti hipotezę (Kardelis, 2022).

Kokybiniam tyrimui atlikti buvo susisiekta su 8 pasirinktais ekspertais. Interviu dalyvavę asmenys išsamiai atsakė į pateiktus klausimus ir aiškiai dėstė savo mintis. Kokybinio tyrimo imtis yra 8 asmenys, kurie pasižymi tokiais kriterijais:

- dirba logistikos srityje;
- darbo patirtis ne mažesnė kaip 2 metai;
- užima vadovaujančias pareigas;
- yra įgiję aukštąjį universitetinį išsilavinimą.

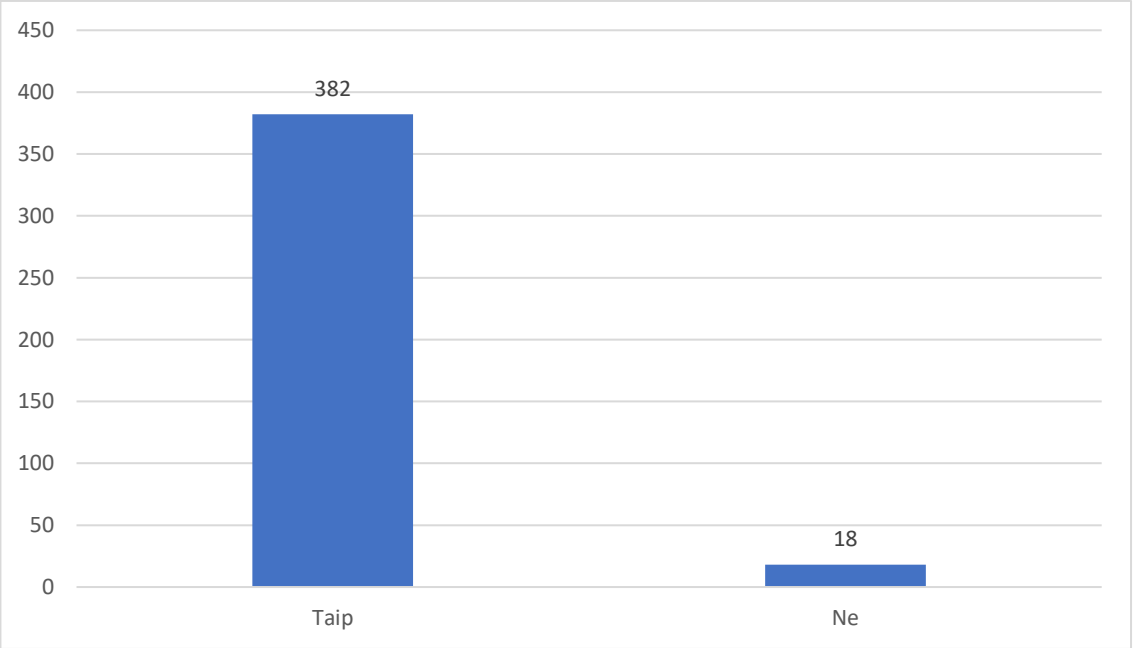
Šios charakteristikos padėjo išgryninti tikslesnius rezultatus, nes ekspertai turi daug patirties logistikos srityje, puikius komunikacinius sugebėjimus, tiksliai bei argumentuotai gali pateikti savo nuomonę į užduodamus klausimus. Kokybinio tyrimo dalyviams buvo suteikti raktiniai pavadinimai: I ekspertas, II ekspertas, III ekspertas ir t. t. (žr. 9 lentelę).

8 lentelė. Pusiau struktūrizuoto ekspertinio interviu ekspertų charakteristikos (sudaryta darbo autorės)

Ekspertas	**Pareigos**	**Darbo trukmė dabartinėse pareigose**	**Išsilavinimas**
I ekspertas	Ekspedijavimo įmonės direktorius	8 metai	Aukštasis universitetinis
II ekspertas	Logistikos įmonės direktorius	9 metai	Aukštasis universitetinis
III ekspertas	Sandėlio vadovas	6 metai	Aukštasis universitetinis
IV ekspertas	Tarptautinių krovinių vežimų skyriaus vadovas	7 metai	Aukštasis universitetinis
V ekspertas	Projektų vadovas	7 metai	Aukštasis universitetinis
VI ekspertas	Informacinių sistemų vadovas logistikos įmonėje	8 metai	Aukštasis universitetinis
VII ekspertas	Kelių transporto vadovas	6 metai	Aukštasis universitetinis
VIII ekspertas	Vietinių vežimų skyriaus vadovas	5 metai	Aukštasis universitetinis

2.4. Kiekybinio tyrimo rezultatai

2023 m. gegužės mėnesį buvo atliktas biometrinių technologijų panaudojimo logistikos procesuose tyrimas, sudaryta 19 klausimų anketinė apklausa (1 priedas), kurią užpildė 400 respondentų. Visi respondentai yra logistikos specialybės studentai arba dirbantys logistikos srityje. Iš pradžių buvo siekiama išsiaiškinti respondentų lytį ir amžių. Iš asmenų, kurie atsakė į šios apklausos klausimus, buvo 198 (49,5 %) moterys ir 202 (50,5 %) vyrai. Apklausoje dalyvavo tik 4 (1 %) respondentai, kuriems yra mažiau nei 20 metų. Dauguma respondentų buvo iki 30 metų amžiaus – 183 (45,75 %) respondentai. 155 (38,75 %) respondentai atitiko amžiaus grupę nuo 30 iki 40 metų, o 50 (12,5 %) respondentų – nuo 40 iki 50 amžiaus intervalą. Taip pat buvo 8 (2 %) respondentai, kurie atitiko nuo 50 iki 60 amžiaus grupę. Šių klausimų atsakymų rezultatai rodo, kad logistikos srityje dirba tiek vyrai, tiek moterys, jie pasiskirstė beveik po lygiai. Šioje apklausoje daugiausiai dalyvavo iki 30 metų amžiaus dirbančių arba besimokančių logistikos srityje apklaustųjų. Apklausoje buvo siekiama išsiaiškinti, kiek respondentų žino ar bent yra girdėję apie biometrines technologijas ir jų galimybes. 390 (97,5 %) respondentų atsakė, kad yra girdėję apie biometrines technologijas ir jų panaudojimą įvairiose srityse, o 10 (2,5 %) – išvis nėra apie jas girdėję.

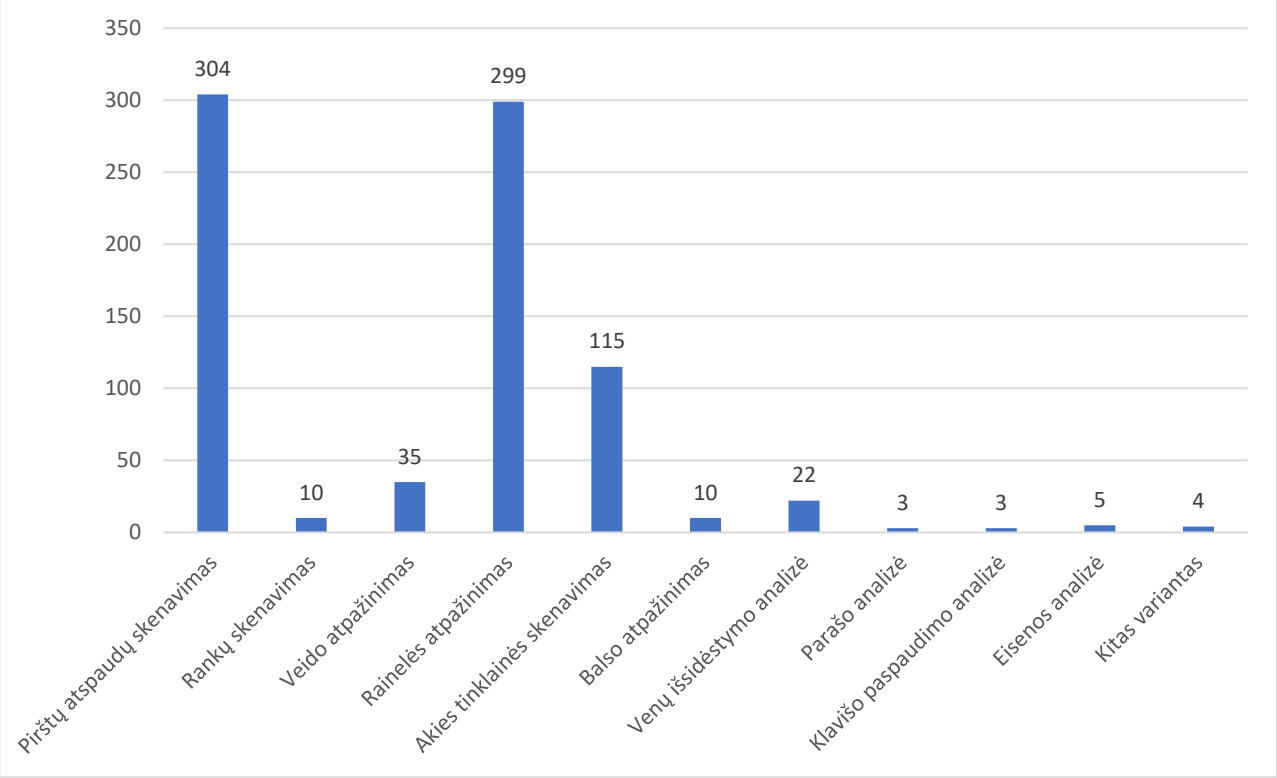


4 pav. Biometrinių technologijų naudojimas (sudaryta darbo autorės)

4 paveiksle galima matyti, kaip pasiskirstė respondentai pagal biometrinių technologijų naudojimą. 382 (95,5 %) respondentai atsakė, kad naudoja biometrines technologijas savo asmeninėje

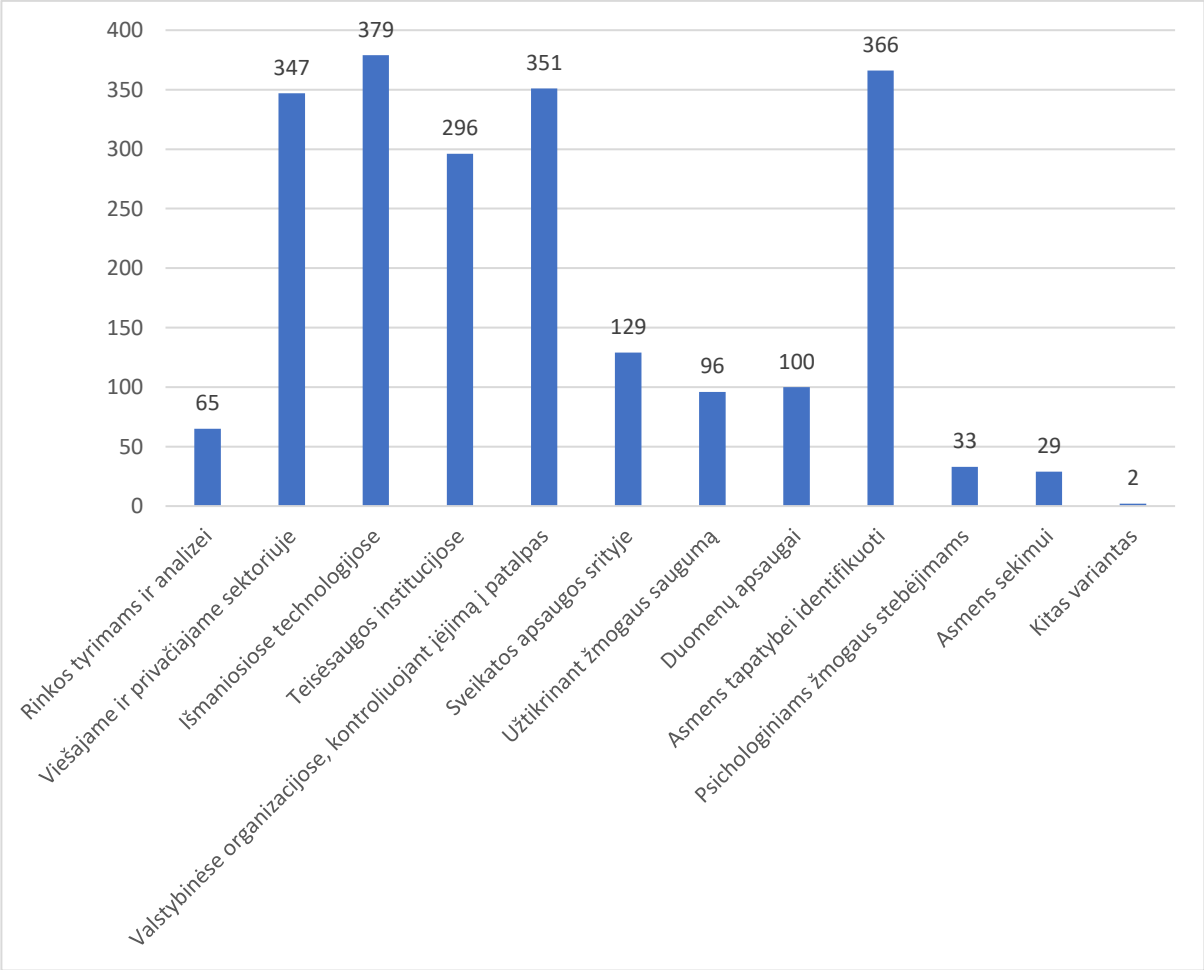
ar darbo aplinkoje, o tik 18 (4,5 %) apklaustųjų – nenaudoja šių technologijų. Dauguma respondentų, biometrines technologijas naudoja savo tapatybės identifikavimui. 318 (79,5 %) respondentų atsakė, kad biometrines technologijas naudoja bankinėse operacijose, 156 (39 %) – sveikatos srityje, o 75 (18,75 %) apklaustieji šias technologijas naudoja savo ar kitų asmenų duomenų apsaugai. Taip pat respondentai minėjo, kad biometrines technologijas jau naudoja išmaniuosiuose telefonuose (pvz., atrakinimui) ir dokumentų pasirašymui.

Kiekviena biometrinių technologijų rūšis turi savo saugumo lygį, priklausomai ar tai fiziologines, ar elgesio ypatybes turinti biometrinė sistema. Respondentai mano, kad pačios saugiausios yra pirštų atspaudų skenavimo ir akies rainelės atpažinimo technologijos (žr. 5 pav.). Šios dvi biometrinių technologijų rūšys yra pačios saugiausios, nes žmogui senstant šie asmens biometriniai duomenys beveik nesikeičia. 115 (28,75 %) apklaustųjų pasirinko, kad saugiausia biometrinių technologijų rūšis yra akies tinklainės skenavimas, o 35 (8,75 %) – veido atpažinimo technologija. Kitos biometrinių technologijų rūšys sulaukė mažiau balsų, galbūt todėl, kad respondentams jos yra mažiau žinomos. Taip pat klausime buvo pateiktas pasirinkimo variantas – kitas variantas. Keli apklaustieji pasirinko šį variantą ir papildė, kad dar galėtų būti saugi DNR analizė, nes jos neįmanoma suklastoti.



5 pav. Saugiausios biometrinės technologijos (sudaryta darbo autorės)

Biometrinės technologijos yra plačiai naudojamos. 6 paveiksle galima matyti respondentų išsidėstymą pagal biometrinių technologijų panaudojimo sritis. 379 (94,75 %) apklaustieji mano, kad biometrines technologijas galima panaudoti išmaniosiose technologijose, 366 (91,5) – asmens tapatybės identifikavimui, o 351 (87,75) apklaustasis pasirinko duomenų apsaugoje ir įmonėms, kurios įėjimą į pastatą kontroliuoja biometrinės technologijos. Taip pat 347 (86,75 %) respondentai mano, kad šias technologijas galima panaudoti privačiajame ir viešajame sektoriuje. 296 (74 %) apklaustieji teigia, kad šias technologijas taip pat galima naudoti net teisėsaugos institucijose, o 96 (24 %) – užtikrinant žmogaus saugumą. Mažiausiai balsų surinko asmens sekimas bei žmogaus elgesio stebėjimai, kurie yra mažiau paplitę ir mažiau žinomi žmonėms. Apibendrinus galima teigti, kad biometrines technologijas galima naudoti visose srityse, kur yra įtraukiami žmonių biometriniai duomenys.



6 pav. Biometrinių technologijų panaudojimo sritys (sudaryta darbo autorės)

Kiekviena įmonė turėtų skirti nemažai dėmesio į paslaugų kokybės gerinimą. Dažnai įmonėse pasitaiko žmogiškojo faktoriaus klaidos darbo metu, kurių išvengti gali padėti technologijų integravimas į įmonės veiklą. Apklausoje 377 (94,25 %) apklaustieji mano, kad naudojant biometrines technologijas, būtų galima sumažinti žmogiškųjų klaidų skaičių, tačiau 9 teigia, kad šios technologijos nepadeda sumažinti klaidų skaičiaus. 14 (3,5 %) apklaustųjų tiesiog nežino. Net 388 (97 %) respondentai sutinka su tuo, kad biometrinių technologijų naudojimas gali suteikti daugiau saugumo bei pagerinti teikiamų paslaugų kokybę, tačiau 12 (3 %) apklaustųjų mano, kad biometrinės technologijos nesuteikia daugiau saugumo ir nepagerina paslaugų kokybės lygio.

Logistikos įmonės, naudojančios biometrines technologijas, turi daug pranašumų. Apklaustieji teigė, kad naudojant biometrines technologijas, įmonės klientams atrodo išmanesnės, rimtesnės ir teikiančios kokybiškesnes paslaugas už kitas įmones. Tai pritraukia klientų dėmesį, nes tai suteikia darbui sklandumo, mažesnį klaidų kiekį, mažiau popierizmo, saugesnį bei greitesnį darbą. Biometrinės technologijos padeda stebėti greitą ir kokybišką krovinių sekimą, užtikrina informacijos privatumą, nes apsaugo dokumentus bei patalpas nuo pašalinių asmenų patekimo ir užtikrina priėjimą prie krovinių tik tų asmenų, kurie turi tam teisę. Respondentai apklausoje minėjo, kad biometrinės technologijos padeda sutaupyti daugiau laiko už įvedamus slaptažodžius. Biometrinės technologijos padeda didinti konkurencinį pranašumą ir palengvina logistinius procesus, o klientai bei darbuotojai gali jaustis saugesni. Tačiau vienas apklaustasis paminėjo, kad nemato prasmės naudoti biometrinių technologijų, nes tam reikia skirti nemažai investicijų. Tas tikrai taip, bet reikėtų įvertinti visas galimybes ir pridėtinę vertę prieš diegiant šias technologijas.

2.5. Kokybinio tyrimo rezultatai

2023 m. spalio mėnesį buvo atliktas biometrinių technologijų panaudojimo logistikos srityje ekspertinis interviu (2 priedas). Buvo pateikti 9 komponentai, kuriuos padėjo išskirti anketinės apklausos respondentai: konkurencingumas (C1), prieigos kontrolė (C2), intelektinės transporto sistemos (C3), saugumas (C4), darbuotojo ir transporto priemonės stebėjimas realiuoju laiku (C5), darbuotojo sveikatos stebėjimas (C6), technologijų patikimumas (C7), mažesnė žmogiškųjų klaidų galimybė (C8), mažesnė įsilaužimų ir vagysčių atvejų tikimybė (C9). Šiuos komponentus ekspertai turėjo suranguoti balais pateiktoje lentelėje nuo 0 iki 4 (žr. 7 lentelę), kurie padėjo išanalizuoti priežastinius ryšius tarp komponentų. Iš viso buvo apklausti 8 ekspertai, kurie atitiko iš anksto nusistatytus kriterijus.

Kaip minėta anksčiau, tyrimui pasirinktas DEMATEL metodas. Taikant šį metodą, buvo išskirti 5 etapai.

1 etapas. Pirmajame etape priežastiniams ryšiams nustatyti, atliktas ekspertų vertinimas balais, kurie aprašyti anksčiau. 10 lentelėje pateikiamas vieno iš ekspertų rangavimas.

9 lentelė. Vieno iš ekspertų atliktas rangavimas (sudaryta darbo autorės)

	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**
C1	-	3	4	4	2	2	4	4	3
C2	4	-	4	4	0	0	0	3	4
C3	3	4	-	4	0	0	0	4	0
C4	4	4	4	-	4	3	4	3	4
C5	3	0	0	4	-	0	0	2	1
C6	2	0	0	2	0	-	0	2	0
C7	4	0	0	4	0	0	-	4	4
C8	4	3	4	3	2	2	4	-	4
C9	3	4	0	4	1	0	4	4	-

2 etapas. Norint išanalizuoti surinktus duomenis, reikia sujungti visų ekspertų rangavimus į vieną lentelę. 11 lentelėje buvo išvestas duomenų aritmetinis vidurkis. Dešinėje buvo įterptas dar vienas stulpelis, kuriame yra pateiktos susistemintų balų sumos ir išrinkta didžiausia sumos reikšmė.

10 lentelė. Susisteminti ekspertų vertinimai (sudaryta darbo autorės)

	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**Suma:**
C1	-	2	3	4	2	3	4	3	4	25
C2	3	-	4	4	2	2	3	3	4	25
C3	2	4	-	4	2	3	3	4	2	24
C4	4	4	4	-	3	3	4	3	4	**29**
C5	3	2	2	3	-	2	3	3	2	20
C6	3	3	3	2	2	-	3	3	1	20
C7	4	3	3	4	3	3	-	4	3	27
C8	3	3	4	3	3	3	4	-	2	25
C9	4	4	2	4	2	1	3	2	-	22

3 etapas. Iš gautų susistemintų duomenų buvo sudaryta tiesioginio ryšio matricą X (žr. 12 lentelę).

11 lentelė. Tiesioginio ryšio matrica X (sudaryta darbo autorės)

X	C1	C2	C3	C4	C5	C6	C7	C8	C9
C1	-	0.069	0.103	0.138	0.069	0.103	0.138	0.103	0.138
C2	0.103	-	0.138	0.138	0.069	0.069	0.103	0.103	0.138
C3	0.069	0.138	-	0.138	0.069	0.103	0.103	0.138	0.069
C4	0.138	0.138	0.138	-	0.103	0.103	0.138	0.103	0.138
C5	0.103	0.069	0.069	0.103	-	0.069	0.103	0.103	0.069
C6	0.103	0.103	0.103	0.069	0.069	-	0.103	0.103	0.034
C7	0.138	0.103	0.103	0.138	0.103	0.103	-	0.138	0.103
C8	0.103	0.103	0.138	0.103	0.103	0.103	0.138	-	0.069
C9	0.138	0.138	0.069	0.138	0.069	0.034	0.103	0.069	-

4 etapas. Pagal tiesioginio ryšio matricą X buvo gauta bendroji ryšių matrica T. Ši matrica yra pateikta 13 lentelėje.

12 lentelė. Bendro ryšio matrica T (sudaryta darbo autorės)

T	C1	C2	C3	C4	C5	C6	C7	C8	C9
C1	-0.063	0.012	0.060	0.095	0.025	0.071	0.097	0.059	0.109
C2	0.055	-0.062	0.102	0.092	0.027	0.030	0.053	0.059	0.106
C3	0.016	0.102	-0.061	0.100	0.029	0.071	0.055	0.104	0.025
C4	0.089	0.091	0.094	-0.079	0.062	0.064	0.088	0.047	0.098
C5	0.068	0.031	0.028	0.066	-0.037	0.037	0.065	0.071	0.034
C6	0.072	0.074	0.068	0.023	0.040	-0.038	0.066	0.067	-0.007
C7	0.094	0.054	0.051	0.090	0.065	0.065	-0.070	0.098	0.060
C8	0.058	0.059	0.102	0.050	0.070	0.068	0.098	-0.061	0.026
C9	0.105	0.111	0.021	0.099	0.038	-0.006	0.060	0.026	-0.055

5 etapas. Šiame etape buvo apskaičiuotos komponentų eilučių ir stulpelių sumos reikšmės (t.y. R ir C reikšmės), kurios yra pateiktos 14 lentelėje. Šios reikšmės leis toliau nustatyti komponentų eiliškumą svarbos tvarka ir komponentų pasiskirstymą pagal priežasčių bei pasekmių grupes.

13 lentelė. Matrica T su apskaičiuotomis R ir C reikšmėmis (sudaryta darbo autorės)

T	C1	C2	C3	C4	C5	C6	C7	C8	C9	R
C1	-0.063	0.012	0.060	0.095	0.025	0.071	0.097	0.059	0.109	0.464
C2	0.055	-0.062	0.102	0.092	0.027	0.030	0.053	0.059	0.106	0.463
C3	0.016	0.102	-0.061	0.100	0.029	0.071	0.055	0.104	0.025	0.443
C4	0.089	0.091	0.094	-0.079	0.062	0.064	0.088	0.047	0.098	0.554
C5	0.068	0.031	0.028	0.066	-0.037	0.037	0.065	0.071	0.034	0.363
C6	0.072	0.074	0.068	0.023	0.040	-0.038	0.066	0.067	-0.007	0.365
C7	0.094	0.054	0.051	0.090	0.065	0.065	-0.070	0.098	0.060	0.508
C8	0.058	0.059	0.102	0.050	0.070	0.068	0.098	-0.061	0.026	0.469
C9	0.105	0.111	0.021	0.099	0.038	-0.006	0.060	0.026	-0.055	0.398
C	0.494	0.472	0.465	0.534	0.320	0.362	0.513	0.471	0.397	

Toliau buvo apskaičiuotos R+C ir R-C reikšmės (žr. 15 lentelę). R+C reikšmės rodo komponentų eiliškumą svarbos tvarka. Kuo didesnė reikšmė, tuo komponentas yra svarbesnis. R-C reikšmės rodo, kurie komponentai yra sukeliantys, o kurie paveikti komponentai. Teigiamos reikšmės rodo, kurie komponentai priklauso priežasties grupei, o neigiamos reikšmės – pasekmių grupei. Galima matyti, kad ekspertinio interviu ekspertai išskyrė pačią svarbiausią biometrinių technologijų savybę logistikos srityje, tai būtų saugumas.

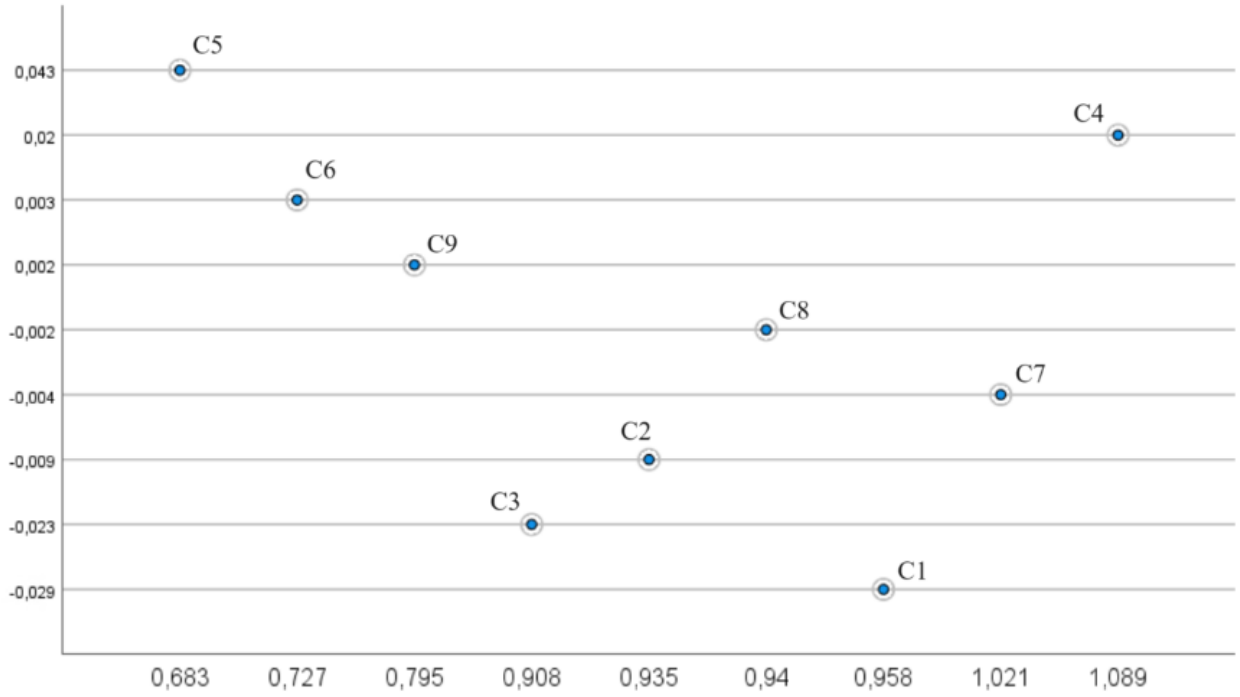
14 lentelė. R+C ir R-C reikšmės (sudaryta darbo autorės)

	C1	C2	C3	C4	C5	C6	C7	C8	C9
R+C	0.958	0.935	0.908	1.089	0.683	0.727	1.021	0.940	0.795
R-C	-0.029	-0.009	-0.023	0.020	0.043	0.003	-0.004	-0.002	0.002
Eiliškumas	3	5	6	1	9	8	2	4	7

Remiantis 15 lentelės duomenimis, galima išskirti komponentus, kurie priklauso priežasčių, o kurie pasekmių grupei. Šie komponentai priklauso priežasčių grupei: saugumas (C4), darbuotojo ir transporto priemonės stebėjimas realiuoju laiku (C5), darbuotojo sveikatos stebėjimas (C6) bei mažesnė įsilaužimų ir vagysčių atvejų tikimybė (C9). Komponentai, turintys neigiamas reikšmes priklauso pasekmių grupei: konkurencingumas (C1), prieigos kontrolė (C2), intelektinės transporto sistemos (C3), technologijų patikimumas (C7) ir mažesnė žmogiškųjų klaidų galimybė (C8).

Komponentų eiliškumas svarbos tvarka išsidėstė taip:

1. saugumas (C4);
2. technologijų patikimumas (C7);
3. konkurencingumas (C1);
4. mažesnė žmogiškųjų klaidų galimybė (C8);
5. prieigos kontrolė (C2);
6. intelektinės transporto sistemos (C3);
7. mažesnė įsilaužimų ir vagysčių atvejų tikimybė (C9);
8. darbuotojo sveikatos stebėjimas (C6);
9. darbuotojo ir transporto priemonės stebėjimas realiuoju laiku (C5).



7 pav. Komponentų priežastiniai ir pasekmių ryšiai (sudaryta darbo autorės)

7 paveiksle pateikta duomenų vizualizacija pagal R+C ir R-C reikšmes. Šis grafikas padeda vizualizuoti ryšius tarp komponentų. Grafike pavaizduota X ašis rodo komponentų svarbos eiliškumą R+C, o Y ašis rodo priežasčių ir pasekmių grupes, kurios yra nustatomos pagal R-C reikšmes.

2.6. Tyrimų apibendrinimas

Apibendrinant šį skyrių galima teigti, kad biometrinių technologijų panaudojimas logistikos srityje gali užtikrinti efektyvesnį darbą ir aukštesnį saugumo lygį. Norint stabiliau įsitvirtinti rinkoje, didinti klientų skaičių bei vežimų apimtis, reikia moderniosios logistikos ir laikui bėgant ją vis tobulinti. Galima pastebėti, kad šiandieniniame pasaulyje svarbų vaidmenį atlieka išmaniosios technologijos, kurios padeda taupyti laiką, išlaidas, didina ir efektyvina darbo našumą.

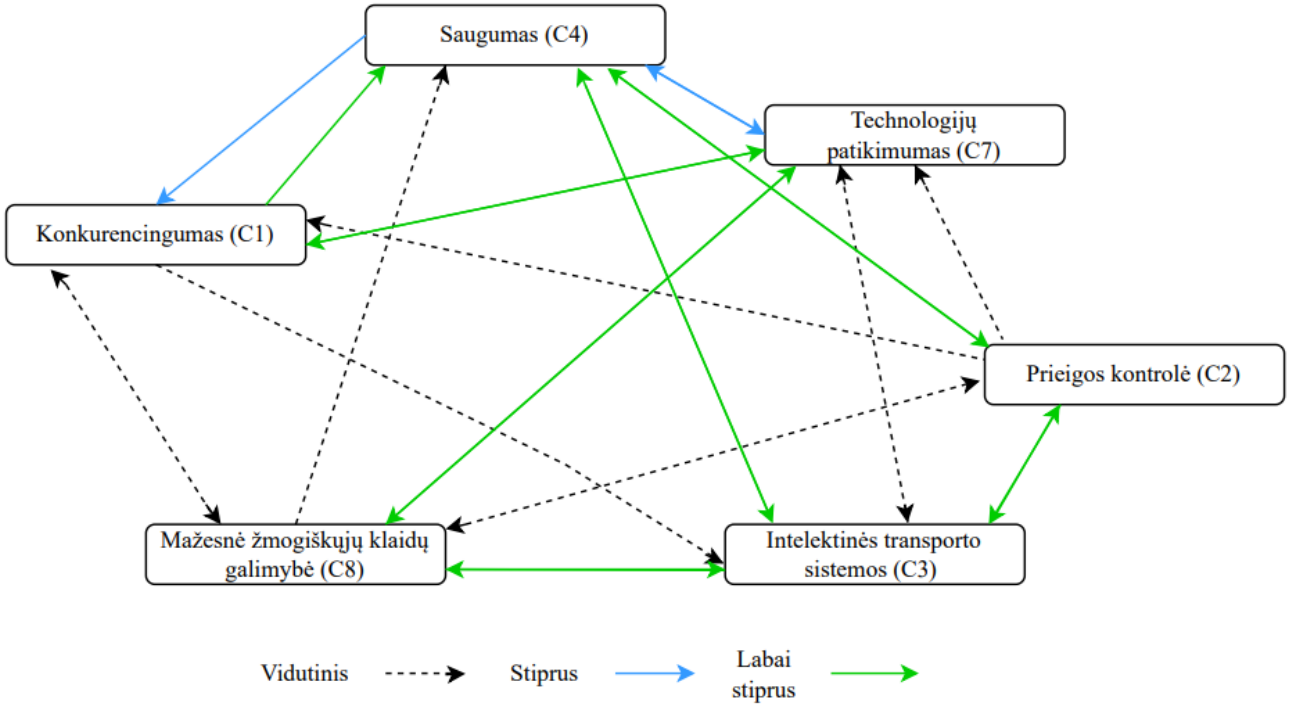
Atlikus biometrinių technologijų panaudojimo anketinės apklausos analizę, dauguma respondentų mano, kad šios technologijos sukuria didelį pranašumą prieš kitas įmones, nes įmonė tampa modernesnė, patikimesnė, galinti pasiūlyti kokybiškesnes paslaugas. Taip pat respondentai išreiškė savo nuomonę, kad biometrinės technologijos yra saugesnės ir patikimesnės už ranka įvedamus slaptažodžius bei RFID technologijas, nes jas sunku nulaužti. Respondentų apklausos rezultatai parodė, kad pačios saugiausios biometrinių technologijų rūšys yra akies rainelės skenavimo ir piršto atspaudo skenavimo sistemos. Iš apklausos duomenų buvo išskirti pagrindiniai biometrinių technologijų privalumai: konkurencingumas (C1), prieigos kontrolė (C2), intelektinės transporto sistemos (C3), saugumas (C4), darbuotojo ir transporto priemonės stebėjimas realiuoju laiku (C5), darbuotojo sveikatos stebėjimas (C6), technologijų patikimumas (C7), mažesnė žmogiškųjų klaidų galimybė (C8), mažesnė įsilaužimų ir vagysčių atvejų tikimybė (C9).

Atliekant kokybinį tyrimą, ekspertai priskyrė atitinkamus balus išskirtiems komponentams. Pagal tuos balus, buvo pritaikytas DEMATEL metodas, kuris padeda nustatyti ryšius tarp komponentų. Atlikus šį metodą, buvo gautas toks rezultatas, kad pats svarbiausias komponentas yra saugumas. Taip pat priežastinius ryšius galima vizualizuoti strateginiame žemėlapyje (žr. 8 pav.), kuris struktūrizuoja ir padeda lengviau matyti komponentų tarpusavio ryšius. Norint strateginiame žemėlapyje atvaizduoti tik reikšmingus ryšius, buvo nustatyta ribinė vertė. Ji buvo apskaičiuota pagal bendro ryšio matricos T visų duomenų vidurkį. Nustatyta ribinė vertė 0.05. Visi komponentai, kurie turi mažesnę reikšmę už ribinės vertės skaitinę reikšmę, nebuvo įtraukti į strateginį žemėlapį, t. y. C5, C6 ir C9.

Norint dar aiškiau pateikti komponentų ryšius strateginiame žemėlapyje, buvo išskirti 3 ryšių lygiai:

- nuo 0,05 iki 0,07 turi vidutinį ryšį;
- nuo 0,071 iki 0,09 turi stiprų ryšį;
- nuo 0,091 iki 0,11 turi labai stiprų ryšį.

Kiekvienam ryšiui buvo priskirtas skirtingas žymėjimo būdas. Vidutinio stiprumo ryšys pažymėtas punktyrine rodykle, stiprus ryšys pažymėtas vientisa mėlyna rodykle, o labai stiprus ryšys – žalia rodykle. Reikšmės, kurios neįtilpo į šiuos tris intervalus, strateginiame žemėlapyje nebuvo pavaizduotos. Taip pat galima matyti dvipuses rodykles, kurios rodo abipusią įtaką.



8 pav. Strateginis žemėlapis, kuris rodo ryšius tarp komponentų (sudaryta darbo autorės)

Strateginiame žemėlapyje pavaizduoti 6 komponentai (C1, C2, C3, C4, C7, C8), kurie savo skaitine reikšme nėra mažesni už ribinę vertę. Likusieji turi mažesnę reikšmę, dėl to jų ryšys silpnas. Taip pat strateginiame žemėlapyje galima įžvelgti, kad stipriausiu ryšiu su kitais komponentais pasižymi saugumas. Tai rodo, kad saugumas yra labai svarbus, naudojant biometrines technologijas. Saugumas taip pat buvo akcentuojamas ir mokslinės literatūros analizėje. Ne ką mažiau yra svarbūs ir kiti komponentai, parodyti strateginiame žemėlapyje. Intelektinės transporto sistemos yra svarbios, nes technologijos yra didelė šio pasaulio dalis, kurios padeda žmonėms planuoti, taupyti finansines ir darbo sąnaudas. Labai svarbu, kad naudojamos technologijos būtų patikimos, nes kitaip įmonei grali kilti grėsmės, tokios kaip klaidos, didėjančios laiko ir finansinės sąnaudos ar konfidencialios informacijos atskleidimas. Apibendrinant abu tyrimus, galima teigti, kad logistikos įmonės efektyvumo gerinimui ir konkurencinio pranašumo didinimui padėtų biometrinių technologijų panaudojimas logistikos srityje.

3. LOGISTIKOS PROCESŲ TOBULINIMO MODELIS PANAUDOJANT BIOMETRINES TECHNOLOGIJAS

3.1. Siūlomas modelis

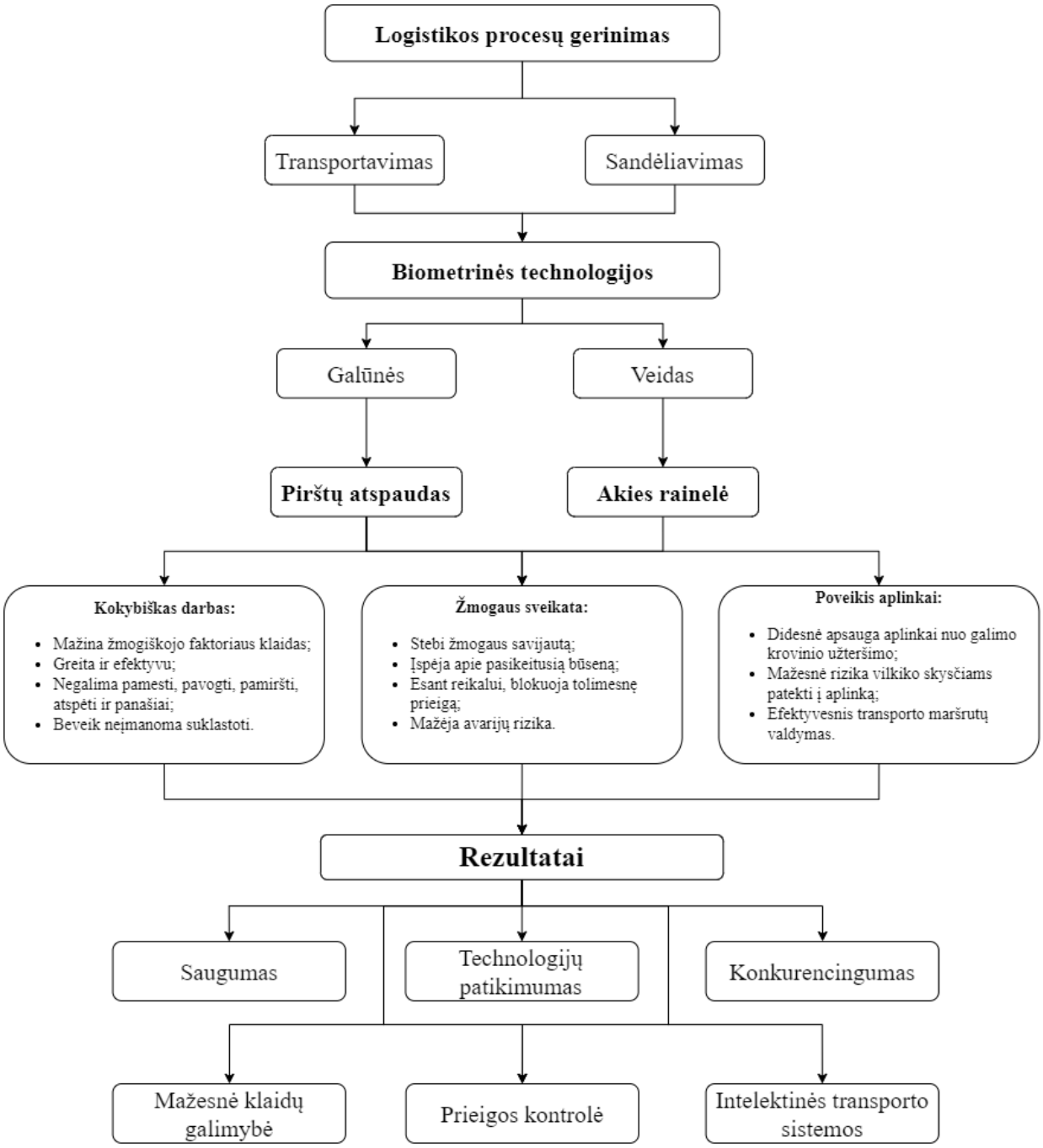
Logistikos sektoriuje greitai besivystančios technologijos tampa esminėmis efektyvumo ir saugumo didinimo priemonėmis. Šiuo kontekstu siūlomas modelis, kuris apima biometrines technologijas logistikos srityje. Išanalizavus biometrinių technologijų mokslinę literatūrą ir jų panaudojimą logistikos srityje, pastebėta, kad tai yra visai nauja sritis logistikos srityje bei teorinės medžiagos nėra labai daug. Naujų technologijų panaudojimas ir jų nuolatinis tobulinimas paverčia įmonę patrauklesne ir padeda labiau įsitvirtinti rinkoje. Galima teigti, kad siūlomas modelis, kuris rodo, kur ir kokios biometrinės rūšys gali būti diegiamos logistikos srityje, atspindi kaip biometrinės technologijos būtų iki galo išnaudotos bei atneštų didžiausią vertę.

Siūlomas modelis rodo logistikos procesus, kuriems tam tikros biometrinių technologijų rūšys galėtų daryti didžiausią įtaką. Rodo, kur ir ką geriausia būtų integruoti į logistikos procesus. Modelyje yra pateiktos tik tos sritys, kuriose biometrinės technologijos turi didžiausią įtaką logistikoje. Remiantis tyrimų rezultatais, kurie buvo atlikti antrajame skyriuje, modelyje pavaizduotos 2 biometrinių technologijų rūšys ir atrinkti 6 svarbiausi komponentai, kuriuos išrangavo logistikos srities ekspertai. Siūlomas modelis, įdiegus biometrines technologijas logistikos srityje, ne tik skatina saugumą, bet ir didina efektyvumą bei pagerina kliento patirtį. Integracija šių technologijų tampa ne tik logistikos procesų gerinimo, bet ir perspektyvaus transporto bei prekybos sprendimų dalimi.

Modelis yra struktūrizuotas ir supaprastintas atvaizdavimas pagal atliktų tyrimų rezultatus, kuris padeda aiškiau suprasti tam tikro reiškinio esmę. Modelyje siūlomos biometrinės technologijos gali būti svarbus įrankis logistikos srityje, siekiant gerinti saugumą, identifikaciją, kontrolę ir operacijų efektyvumą. Biometrinių technologijų integracija siekiama pagerinti logistikos procesų efektyvumą ir greitį. Šios technologijos gali sukurti patogesnę, saugesnę ir greitesnę logistikos paslaugų naudojimo patirtį tiek darbuotojams, tiek krovinių gabenimo klientams.

Būtina atsižvelgti į specifinius įmonės poreikius ir operacijų sritis, kad būtų pasirinkti tinkamiausi sprendimai ir diegiamos efektyvios biometrinės technologijos. Tinkamai pasirinkti logistikos procesai ir tinkamos biometrinių technologijų rūšys gali sumažinti vagysčių, nelegalios veiklos, laiko sąnaudų, finansinių išlaidų ir kitų saugumo rizikų pavojų.

Anksčiau darbe pavaizduotas teorinis modelis buvo patobulintas pagal atliktų tyrimų rezultatus (žr. 9 pav.).



9 pav. Modelis, rodantis biometrinių technologijų integraciją į logistikos procesus (sudaryta darbo autorės)

Sudarant 9 paveiksle pavaizduotą modelį, išskirti pagrindiniai logistikos procesai, kuriuose biometrinės technologijos darytų didžiausią įtaką: transportavimui ir sandėliavimui. Norint efektyviai

pritaikyti biometrines technologijas, neužtenka išsirinkti tik taikomą sritį. Taip pat reikėtų atsirinkti tas biometrinių technologijų rūšis, kurios geriausiai pritaikomas tose srityse. Biometriniai duomenys naudojami identifikuoti asmenis logistikos grandinėje. Tai apima, vairuotojus ir kitus darbuotojus, kurie dalyvauja logistikos procesuose. Biometrinės technologijos, tokios kaip piršto antspaudų atpažinimas ir akių rainelės skenavimas, gali pasiūlyti išskirtinę vertę siūlomuose logistikos procesuose. Šios biometrinių technologijų rūšys yra pačios saugiausios ir patikimiausios, nes jų beveik neįmanoma suklastoti.

Buvo išskirti 3 aspektai, kuriems biometrinės technologijos turi poveikį: poveikis aplinkai, žmogaus sveikatai ir darbui. Biometrinės technologijos padeda užtikrinti kokybiškesnį darbą, kaip jau buvo minėta anksčiau, nes padeda sumažinti žmogiškojo faktoriaus klaidas. Tai turi teigiamą poveikį darbo kokybei. Biometrinės technologijos užtikrina greitesnį, efektyvesnį ir tikslesnį darbą. Naudojant šias technologijas, yra padidinamas saugumas, kadangi jos yra unikalios ir jų beveik neįmanoma suklastoti, tuo labiau pamesti ar pavogti. Taip pat biometrinės technologijos padeda stebėti žmogaus sveikatą ir tai užtikrina dar didesnę darbo saugą, saugant darbuotojo sveikatą ir mažinant avarijų galimybių skaičių. Naudojamos biometrinės technologijos padeda saugoti aplinką, sumažindamos gamtos užterštumą nuo transporto priemonių skysčių ar pavojingų krovinių išsiliejimo. Iš to išeina prielaidos, kad biometrinės technologijos padeda stebėti darbuotojus, jų darbo laiką ir būseną, kontroliuoti pašalinių asmenų patekimą į patalpas ar transporto priemonių prieigą, taip padeda sumažinti sukčiavimų ir vagysčių atvejų. Taip pat šios technologijos užtikrina sklandų informacijos sklidimą per esamus jutiklius.

Ekspertų atliktas rangavimas padėjo atrinkti pačius svarbiausius komponentus jų nuomone, kitaip tariant, biometrinių technologijų privalumus. 6 patys svarbiausi komponentai buvo pavaizduoti modelyje kaip rezultatai: saugumas, technologijų patikimumas, konkurencingumas, mažesnė klaidos galimybė, prieigos kontrolė ir intelektinės transporto sistemos. Pagal gautus rezultatus, labiausiai biometrines technologijas verta diegti dėl saugumo. Biometrinės technologijos gali prisidėti prie didesnio saugumo dėl kelių priežasčių. Visų pirma, biometrinės technologijos naudoja žmogaus duomenis, kurie yra unikalūs kiekvienam asmeniui, todėl biometrinės identifikavimo sistemos gali pasiūlyti aukštesnį duomenų apsaugos lygį. Taip pat sumažina galimybę, kad nepageidaujamas žmogus galės pasinaudoti kieno nors kito tapatybe, nes slaptažodžiai ir užmirštamos RFID kortelės gali sukelti saugumo spragas. Tačiau reikia pabrėžti, kad biometrinės technologijos taip pat turi savų iššūkių. Tai apima galimas technologijos klaidas arba klaidingus atpažinimus. Todėl, nors biometrinės technologijos gali pagerinti saugumą, svarbu jas naudoti atsakingai.

3.2. Modelio aprobavimas

Biometrinės technologijos, plintančios sparčiu tempu, atveria naujas galimybes saugumo ir žmogaus identifikavimo srityse. Modelio aprobavimas biometrinių technologijų kontekste yra išties esminis etapas, siekiant įvertinti modelio tinkamumą, patikimumą ir galimą plėtros potencialą. Tai bus siekiama nustatyti ekspertinio interviu metodu, ką ekspertai mano apie biometrinių technologijų panaudojimo galimybes logistikos srityje bei siūloma modelį. Šis metodas leidžia pritaikyti žmonių, kurie turi daug žinių, patirties ir kompetencijos analizuojamoje temoje, įvertinimą.

Ekspertinis interviu metodas leido nustatyti, kad ekspertų nuomonė biometrinių technologijų klausimu yra vieninga. Dauguma ekspertų teigė, kad biometrinės technologijos yra nauja tema logistikoje, tačiau mano, kad jos turi potencialo didesnėse įmonėse, nes vis dėlto reikalauja investicijų. Visi sutinka, jog išmaniosios technologijos yra neatsiejama mūsų gyvenimo dalis ir perspektyvos, jos nuolat tobulės, lems darbo pobūdžio kaitą, privers prisitaikyti prie besikeičiančių sąlygų ir nuolat ieškoti naujų sprendimų. Biometrinės technologijos nėra išimtis. Jų integravimas į logistikos procesus gali reikšmingai sumažinti procesų atlikimo laiką ir žmogiškojo faktoriaus klaidų riziką. Pavyzdžiui, vienas iš respondentų pateikė pavyzdį, kad „biometrinės technologijos padėtų sustiprinti užtikrintumą, kad tik tie darbuotojai, kurie turi leidimą, galėtų prieiti prie krovinio, patalpų, informacinių sistemų ir transporto priemonių“. Biometrinė sistema anuliuotų galimybę pašaliniams asmenims prieiti prie krovinio. Todėl galima teigti, kad biometrinės technologijos suteikia unikalios tapatybės patvirtinimą, mažina sukčiavimo riziką ir optimizuoja prieigą prie logistikos procesų. Biometrinė sistema yra skirta saugiam krovinio pristatymui, apsaugoti nuo krovinių praradimų ir vagysčių. Visa ši sistema yra automatizuota, todėl klientams įmonė su biometrine sistema atrodo patrauklesnė, nes užtikrina didelį saugumą ir privatumą. O ypač aktualu didelės vertės krovinius turinčiai įmonei. Juk klientui tai yra taip pat pridėtinė vertė, nes jis yra suinteresuotas, kad jo prekės atvyktų kaip įmanoma saugiau.

Apimant biometrinių technologijų rūšis, visi ekspertai paminėjo pirštų ir akių atpažinimą, nes šios biometrinių technologijų rūšys būtų pačios patogiausios naudoti norint patekti į patalpą ir prieigai prie transporto priemonių. Trumpai apžvelgiant šias biometrinių technologijų rūšis, tai jos yra pačios saugiausios, tiksliausios, patogiausios naudotis ir jas sunku suklastoti. O ir bėgant laikui šie asmens biometriniai duomenis nesikeičia, dėl ko nėra būtini duomenų atnaujinimai.

Vienas ekspertas interviu metu akcentavo būtent darbuotojo būklės stebėjimą. Tai leistų įvertinti ir nuolatos stebėti darbuotojų sveikatą, fizinę ir psichologinę būklę. Stebima žmogaus būsena leistų išvengti darbuotojo pervargimo, klaidų ir avarijų rizikos. Ekspertas teigia, kad „biometrinės

technologijos galėtų atpažinti ne tik blaivumą, bet ir bendrą savijauta, pavyzdžiui, ar darbuotojas nekarščiuoja“. Vairuotojo būklės stebėjimas yra be galo svarbus. Biometrinė sistema galėtų užtikrinti, kad vairuotojai už vairo sėstųsi tik blaivi, neprisivartoję psichotropinių vaistų ar kitų medžiagų, pakankamai pailsėję ir esant reikalui, blokuotų transporto priemonės užvedimo sistemą. Biometrinių technologijų sistema, identifikavusi vairuotojo nuovargį, galėtų jį įspėti ir nukreipti į artimiausią stovėjimo aikštelę. Darbuotojo būklės stebėjimas galėtų galioti ir sandėlininkams, nes net keli respondentai teigė, kad vakarais, laukiant vėluojančių vilkikų, išgeria alkoholinių gėrimų. Vienas ekspertas teigia, kad „darbuotojo sveikatos stebėjimas ir mažesnė žmogiškųjų klaidų galimybė įtakotų nelaimingų atsitikimų skaičiaus mažėjimą“.

Nelaimingų atsitikimų skaičiaus mažinimas prisideda ir prie gamtos užterštumo mažinimo. Juk dažnai pasitaiko, kai avarijų metu į gamtą išsilieja transporto priemonės skysčiai arba pažeisti kroviniai. Taip pat ekspertai teigė, kad biometrinių technologijų naudojimas padėtų sumažinti poreikį naudoti popierių, plastikines atmintines, korteles ir kitus panašius reikmenis. Tai mažintų popieriaus ir plastiko gamybos kiekius, jų atliekų kiekius. Tai leistų taupyti elektros energijos sunaudojimo kiekius popieriaus ir plastiko gamybai bei naudojimui. Keli ekspertai tvirtino, kad biometrinės technologijos užtikrina efektyvesnį maršrutų valdymą, kuris turi teigiamą poveikį aplinkai, nes leidžia optimizuoti kelią, sumažinti nuvažiuojamą atstumą ir išmetamų teršalų kiekį. Mažiau aplinka teršiama, kai mažiau veiksmų reikia atlikti ir mažiau sunaudoti išteklių procesams atlikti. Taip pat vienas ekspertas užsiminė, kad biometrinės technologijos gali pagerinti sandėliavimo ir inventorizacijos procesus, užtikrinant tikslų ir efektyvų prekių stebėjimą. Tai gali sumažinti perteklinį prekių kiekį, kuris gali lemti mažesnį transporto poreikį.

Apibendrinant ekspertinio interviu rezultatus, galima teigti, kad tai yra nauja tema Lietuvoje, tačiau ekspertai siūlomą modelį vertina teigiamai, tik reikėtų įvertinti diegimo galimybes ir kaštus. Įmonei diegtis šias technologijas būtų tikras iššūkis, nes kol kas tik kelios logistikos įmonės pasaulyje naudoja šias technologijas ir sunkiau būtų remtis kitų įmonių diegimo patirtimi. Įmonė, naudojanti biometrines technologijas, gali padėti išvengti įvairių klaidų, pagerinti krovinių ir terminalų saugumą. Vairuotojų būklės stebėjimas užtikrintų saugesnį kelyje krovinių transportavimą, tai padėtų išvengti nelaimingų atsitikimų skaičių kelyje ir transporto skysčių bei krovinio išsiliejimą į aplinką. Klientas gali būti tikras, kad jo krovinys keliauja saugiai. Visos naujausios technologijos ir jų realizacija įmonės viduje kelia bendrą įmonės konkurencingumą bei garantuoja puikią patirtį, todėl su tokiomis įmonėmis norima dirbti ir ateityje. O jei įmonė pirmoji pradėtų naudoti šias technologijas Lietuvoje, ji įgautų stiprų konkurencinį pranašumą.

IŠVADOS

1. Atlikus mokslinės literatūros analizę, apibrėžta biometrinių technologijų samprata, tai yra technologijų sritis, kuri identifikuoja asmens tapatybę. Naudojant unikalius asmens biometrinius duomenis, biometrinės technologijos tampa patikimesnės ir sumažina žmogiškojo faktoriaus klaidas. Biometrinių technologijų pagrindinis tikslas yra nustatyti asmens tapatybę, užtikrinti krovinių ir žmonių saugumą. Biometriniai duomenys yra skirstomi į fiziologines ir elgesio ypatybes turinčias biometrines technologijas. Biometrinės technologijos yra plačiai naudojamos, jos suteikia didesnį pranašumą prieš konkurentus, nes jos suteikia galimybę stebėti vairuotoją ir gabenamą krovinį, jų būklę, o tai užtikrina geresnę teikiamų paslaugų kokybę. Biometrinės technologijos gali suteikti įdomių galimybių logistikos procesams tobulinti ir modernizuoti.

2. Išanalizavus apklausos rezultatus, galima teigti, kad respondentai biometrinių technologijų naudojimą vertina teigiamai tiek asmeninio naudojimo, tiek darbo aplinkoje. Apklaustieji minėjo, kad biometrinės technologijos padeda didinti konkurencingumo lygį, taupyti laiko sąnaudas, logistikos įmonė klientams atrodo išmanesnė, kuri gali pasiūlyti sklandesnes teikiamas paslaugas. Ekspertinis vertinimas leido identifikuoti esminius komponentus, kuriuos ekspertai laiko svarbiausiais biometrinių technologijų atžvilgiu: saugumas, technologijų patikimumas, konkurencingumas, mažesnė klaidos galimybė, prieigos kontrolė ir intelektinės transporto sistemos. Komponentų tarpusavio ryšiai buvo pavaizduoti strateginiame žemėlapyje. Buvo išskirti 3 ryšių lygiai: nuo 0,05 iki 0,07 vidutinis ryšys, nuo 0,071 iki 0,09 stiprus ryšys ir nuo 0,091 iki 0,11 labai stiprus ryšys. Visi komponentai, kurie turi mažesnę reikšmę už ribinės vertės skaitinę reikšmę, nebuvo įtraukti į strateginį žemėlapį, tai būtų darbuotojo ir transporto priemonės stebėjimas realiuoju laiku, darbuotojo sveikatos stebėjimas bei mažesnė įsilaužimų ir vagysčių atvejų tikimybė. Remiantis gautais rezultatais, išryškėjo, kad pagrindinė priežastis, kodėl būtų naudinga diegti biometrines technologijas, yra saugumo aspektas.

3. Pasiūlytas modelis atskleidžia, kad biometrinės technologijos gali turėti didžiausią poveikį šiems logistikos procesams: transportavimui ir sandėliavimui. Remiantis antrajame skyriuje atliktų tyrimų rezultatais, modelyje pavaizduotos dvi biometrinių technologijų rūšys: pirštų atspaudų ir akies rainelės skenavimas. Modelyje yra pateikiami rezultatai, ką suteiktų naudojamos biometrinės technologijos, t.y. išrinkti šeši pagrindiniai komponentai (saugumas, technologijų patikimumas, konkurencingumas, mažesnė klaidos galimybė, prieigos kontrolė ir intelektinės transporto sistemos), kuriuos logistikos ekspertai laiko esminiais. Modelis, kuris įtraukia biometrines technologijas į logistikos sritį, ne tik skatina saugumą, bet ir padidina operatyvumą bei suteikia geresnę kliento

patirtį. Ekspertai išreiškia teigiamą požiūrį į pasiūlytą modelį, bet pabrėžia būtinybę atidžiau įvertinti diegimo galimybes ir išlaidas. Biometrinių technologijų naudojimas įmonėje gali ne tik padėti išvengti klaidų, bet ir didinti krovinių bei terminalų saugumą. Jos gali būti naudingos didinant tiekimo grandinės saugumą, jeigu biometrinės technologijos yra įdiegiamos atsakingai.

4. Šiame darbe buvo iškelta hipotezė – biometrinės technologijos didina saugumo lygį ir padeda išlaikyti sėkmingai veikiančius tiekimo grandinės procesus. Atlikus kiekybinį ir kokybinį tyrimą, galima patvirtinti šią hipotezę, nes biometrinės technologijos suteikia didesnį saugumo lygį. Pirmiausia, biometrinės technologijos, tokios kaip pirštų atspaudų ar veido atpažinimas, gali stiprinti asmenų identifikaciją, taip sumažindamos galimybę neteisėtai prieigai. Tai gali būti itin svarbu tiekimo grandinėje, kur saugumas ir patikimumas yra pagrindiniai veiksniai. Be to, naudojant biometrinius duomenis, galima sumažinti riziką dėl praradimo ar vagystės, nes biometriniai duomenys yra unikalūs kiekvienam asmeniui. Taip pat biometrinės technologijos gali pagerinti prieigą prie duomenų ir fizinių objektų, padėdamos efektyviau valdyti tiekimo grandinės procesus. Tai gali apimti greitesnį prekių ir paslaugų judėjimą, efektyvesnį stebėjimą, mažesnį galimų klaidų skaičių bei sukčiavimo lygį.

SIŪLYMAI

1. Iš pradžių siūloma įmonei išanalizuoti kiekvienos biometrinių technologijų rūšies privalumus ir trūkumus bei parinkti tinkamiausią. Svarbu iš anksto susidėlioti veikimo planą ir diegimo galimybes, kad būtų galima išnaudoti visas biometrinių technologijų panaudojimo galimybes ir kokybiškai pristatyti klientams.

2. Taip pat siūloma iš anksto nusistatyti kylančias rizikas, kad būtų galima jų išvengti biometrinių technologijų diegimo ir veikimo metu. Reikėtų įvertinti biometrinių technologijų diegimo ir veikimo išlaidas, numatyti finansavimo šaltinį ir skirti dalį pinigų neplanuotoms išlaidoms, kad logistikos įmonė nepatirtų finansavimo trūkumo ir nesustotų biometrinių technologijų naudojimas.

LITERATŪROS SĄRAŠAS

1. Abomhara, M., Yayilgan, S. Y., Nweke, L. O., & Székely, Z. (2021). A comparison of primary stakeholders' views on the deployment of biometric technologies in border management: Case study of Smart mobility at the European land borders. *Technology in Society*, *64*, 101484.

2. *Adoption of biometrics in the automotive industry*. (2017). https://www.frost.com/frost-perspectives/adoption-of-biometrics-in-the-automotive-industry/

3. Akkaya, M., & Kaya, H. (2019). Innovative and smart technologies in logistics. *In 17th International Logistics and Supply Chain Congress*, 97–105.

4. Albilali, E., Aboalsamh, H., & Al-Wabil, A. (n.d.). Comparing brain-computer interaction and eye tracking as input modalities: An exploratory study. *In 2013 International Conference on Current Trends in Information Technology (CTIT)*, 232–236.

5. Alrahawe, E. A. M., Humbe, V. T., & Shinde, G. N. (2021). A Biometric Technology-Based Framework for Tackling and Preventing Crimes. *Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications*, 133–160.

6. Alsaadi, I. M. (2021). Study On Most Popular Behavioral Biometrics, Advantages, Disadvantages And Recent Applications : A Review. *Int. J. Sci. . Technol. Res*, *10*, 15–21.

7. Baldini, G., Geib, F., & Giuliani, R. (2019). Continuous authentication of automotive vehicles using inertial measurement units. *Sensors*, *19*(23), 5283.

8. Bartkienė, L. (2014). Intelektualaus darbo našumo valdymas taikant biometrines technologijas. *(Daktaro disertacija, Vilniaus Gedimino technikos universitetas)*.

9. Bilevičienė, T., & Jonušauskas, S. (2011). *Statistinių metodų taikymas rinkos tyrimuose: vadovėlis.* Vilnius: Mykolo Romerio universitetas.

10. *Biometrics: definition, use cases, latest news*. (2021, June 2). https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

11. Borgianni, Y., Rauch, E., Maccioni, L., & Mark, B. G. (2018). User experience analysis in industry 4.0-the use of biometric devices in engineering design and manufacturing. *In 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)* , 192–196.

12. Ćatović, E., & Adamović, S. (2017). Application of Biometrics in Automotive Industry-Case Study Based on Iris Recognition. *In Sinteza 2017-International Scientific*

Conference on Information Technology and Data Related Research, (pp.44-49). Singidunum University.

13. Choudhary, J. (2012). Survey of different biometrics techniques. *International Journal of Modern Engineering Research (IJMER), ISSN*, 2249–6645.

14. *Darbo rinka Lietuvoje (2022 m. leidimas)*. (2022).

15. Dovydaitis, L. (2018). Lietuviškai kalbančio diktoriaus identifikavimo naudojant rekurentinius neuroninius tinklus tikslumo tyrimas (*Daktaro disertacija, Vilniaus universitetas*).

16. Dytczak, M., & Ginda, G. (2016). DEMATEL-based ranking approaches. *The Central European Review of Economics and Management*, *16*(3), 191–202.

17. Elhennawy, A. P. M., & Amer, M. (2017). Smart Cards Structure and Applications: Emerging and Evolution. *ACS Advances in Computer Science, 11(1), 77–92.*

18. Faundez-Zanuy, M. (2006). Biometric security technology. *IEEE Aerospace and Electronic Systems Magazine*, *21*(6), 15–26.

19. FBI. (2006). *Cargo Theft's High Costs*. Thieves Stealing Billions Annually. https://archives.fbi.gov/archives/news/stories/2006/july/cargo_theft072106

20. Gaižauskaitė, I., & Valavičienė, N. (2016). *Socialinių tyrimų metodai: kokybinis interviu: vadovėlis.* Vilnius: Registrų centras.

21. Galatiltytė, S. (2022). Visuomenės vaistinės farmacijos specialistų nuomonė apie teikiamų paslaugų įtaką pacientų saugumui (*Magistro baigiamasis darbas, Lietuvos mokslų universitetas*).

22. Galterio, M. G., Shavit, S. A., & Hayajneh, T. (2018). A review of facial biometrics security for smart devices. *Computers*, *7*(3), 37.

23. Gayathri, M., Malathy, C., & Prabhakaran, M. (2020). A review on various biometric techniques, its features, methods, security issues and application areas. *In International Conference On Computational Vision and Bio Inspired Computing*, 931–941.

24. Gedminas, T. (2016). Teksto įvedimas naudojant žvilgsnio sekimą. *(Daktaro disertacija, Kauno technologijos universitetas)*.

25. Gomez-Barrero, M., Drozdowski, P., Rathgeb, C., Patino, J., Todisco, M., Nautsch, A., ..., & Busch, C. (2022). Biometrics in the era of COVID-19: challenges and opportunities. *IEEE Transactions on Technology and Society*.

26. Grigaitė, G. (2022). Informacinių technologijų poveikis logistikos sektoriaus įmonių žmogiškųjų išteklių valdymui (*Daktaro disertacija, Vilniaus Gedimino technikos universitetas*).

27. Grünenberg, K., Møhl, P., Olwig, K. F., & Simonsen, A. (2022). Issue Introduction: Identities and Identity: Biometric Technologies, Borders and Migration. *Ethnos*, *87*(2), 211–222.

28. Gutauskaitė, V. (2009). Aeropalinologinės informacijos poreikis: vartotojų nuomonės analizė (*Magistro baigiamasis darbas, Šiaulių universitetas*).

29. Hussain, S. M., Kanakam, P., & Chakravarthy, A. S. N. (2017). Inhibiting Cognitive Bias in Forensic Investigation Using DNA Smart Card with IOT. *International Journal of Control Theory and Applications*, *10*(14), 251–255.

30. Iwuoha, V. C. (2018). ICT and elections in Nigeria: Rural dynamics of biometric voting technology adoption. *Africa Spectrum*, *53*(3), 89–113.

31. Jain, A. K. (2005). Biometric recognition: how do I know who you are? *In International Conference on Image Analysis and Processing*, 19–26. Springer, Berlin, Heidelberg.

32. Jain, A. K., Bolle, R., & Pankanti, S. (2006). Biometrics: personal identification in networked society. In *Springer Science & Business Media* (Vol. 479).

33. Jandl, C., Wagner, M., Moser, T., & Schlund, S. (2021). Reasons and Strategies for Privacy Features in Tracking and Tracing Systems – A Systematic Literature Review. *Sensors 2021*, *21*(13), 4501.

34. Joseph, A. D., Beresford, A. R., Bacon, J., Cottingham, D. N., Davies, J. J., Jones, B. D., & Zhang, J. (2006). Intelligent transportation systems. *IEEE Pervasive Computing*, *5*(4), 63–67.

35. Jurgilas, K. (2021). Dviejų faktorių (2FA) skaitmeninio autentifikavimo metodas nuotolinei prieigai prie kritinės infrastruktūros sistemos. *(Daktaro disertacija, Kauno technologijos universitetas)*.

36. Kačerauskas, T. (2014). Kūrybos visuomenė: tyrimo metodai ir problemos. *LOGOS-A Journal of Religion, Philosophy, Comparative Cultural Studies and Art*, *80*, 6–15.

37. Kaklauskas, A., & Zavadskas, E. K. (2010). *Intelektinė ir biometrinė sprendimų parama*. Vilnius: Technika.

38. Kardelis, K. (2022). Mokslinių tyrimų metodologija ir metodai:(edukologija ir kiti socialiniai mokslai).

39. Kavaliauskaitė, E. (2022). Sumaniųjų technologijų sprendimų taikymas logistikos įmonėse. *In Conference "Young Scientist 2022"* 106–111.

40. Koca, G., & Yıldırım, S. (2021). Bibliometric analysis of DEMATEL method. *Decision Making: Applications in Management and Engineering*, *4*(1), 85–103.

41. Labayen, M., Vea, R., Flórez, J., Aginako, N., & Sierra, B. (2021). Online student authentication and proctoring system based on multimodal biometrics technology. *IEEE Access*, *9*, 72398–72411.

42. Lawton, G. (1998). Biometrics: a new era in security. *Industry Trends, Computer IEEE*, *31*(08), 16–18.

43. Mason, J., Dave, R., Chatterjee, P., Graham-Allen, I., Esterline, A., & Roy, K. (2020). *An Investigation of Biometric Authentication in the Healthcare Environment*. *8*, 100042.

44. Morosan, C. (2016). *Opportunities and challenges for biometric systems in travel: a review*. Travel and Tourism Research Association: Advancing Tourism Research Globally. 61. https://scholarworks.umass.edu/ttra/2011/Oral/61

45. Muralidharan, K., Niehaus, P., & Sukhtankar, S. (2016). Building state capacity: Evidence from biometric smartcards in India. *American Economic Review*, *106*(10), 2895–2929.

46. Olson, R., Thompson, S. V., Wipfli, B., Hanson, G., Elliot, D. L., Anger, W. K., ..., & Perrin, N. A. (2016). Sleep, dietary, and exercise behavioral clusters among truck drivers with obesity: implications for interventions. *Journal of Occupational and Environmental Medicine*, *58*(3), 314.

47. Panischev, O. Y., Ahmedshina, E. N., Talipov, N. G., Katasev, A. S., & Kataseva, D. V. Akhmetvaleev, A. M. Akhmetvaleeva, I. V. (2020). *Adaptive neural network system to build environmental prediction and control by their typing biometrics*. *7*(4), 591–598.

48. Pukėnas, K. (2009). Kokybinių duomenų analizė SPSS programa. Kaunas: Lietuvos kūno kultūros akademija.

49. Rahman, N. A. A., Rosshahdan, A. M., Mohammad, M. F., Majid, Z. A., & Mokhtar, A. Z. (2021). Biometric Technology Application in the Aviation Industry: Preliminary Findings from Passenger Perspective. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(11), 2279–2288.

50. Rivandi, P., Winda, A., Satrio, D., & Solihin, M. I. (2019). Automotive Start–Stop Engine Based on Fingerprint Recognition System. In *E3S Web of Conferences* (Vol. 130, p. 01022).

51. Rudzkienė, V. (2005). Socialinė statistika: vadovėlis. Vilnius: Mykolo Romerio universitetas.

52. Savickas, A. (2008). Biometrija ir asmens duomenų apsauga: teisiniai aspektai (*Magistro baigiamasis darbas, Mykolo Romerio universitetas*).

53. Shamsuzzoha, A., & Helo, P. T. (2011). Real-time tracking and tracing system: Potentials for the logistics network. *In Proceedings of the 2011 International Conference on Industrial Engineering and Operations Management*, 22–24.

54. Thenuwara, S. S., Premachandra, C., & Kawanaka, H. (2022). A multi-agent based enhancement for multimodal biometric system at border control. *Array*, *14*, 100171.

55. Tidikis, R. (2003). Socialinių mokslų tyrimų metodologija: vadovėlis. Vilnius: Lietuvos teisės universitetas.

56. Trukšina, O. (2013). Biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybės užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje (*Magistro baigiamasis darbas, Mykolo Romerio universitetas*).

57. Trukšina, O., & Vasiliauskas, R. (2014). Asmens biometrinių duomenų panaudojimo, nustatant tapatybę biometriniais metodais, teisinio reglamentavimo analizė Lietuvos Respublikoje. *Public Security and Public Order*, *12*.

58. Unar, J. A., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern Recognition*, *47*(8), 2673–2688.

59. Villemure, J., Yeh, P., Policano, R., Kaisser, M., & Gruhn, R. (2018). The Dragon Drive Innovation Showcase: Advancing the State-of-the-Art in Automotive Assistants. *Studientexte Zur Sprachkommunikation: Elektronische Sprachsignalverarbeitung*, 278–284.

60. Vinogradova, I. (2015). Nuotolinių kursų parinkimo optimizavimas (*Daktaro disertacija, Vilniaus universitetas*).

61. Yu, L., & Li, K. (2018). The Design and Implementation of the Intelligent Warehouse Voice Control Guard System Based on Voiceprint Recognition. *In IOP Conference Series: Materials Science and Engineering*, (Vol. 466, No. 1, 012035). IOP Publishing.

62. Yuda, E., Konishi, K., & Takahashi, M. (2021). Evaluation of Physiological and Psychological Stress in Head Driver Leading Self-Driving Truck. *In International Symposium on Affective Science and Engineering ISASE2021*, 1–2.

63. Zheng, T., Glock, C. H., & Grosse, E. H. (2022). Opportunities for using eye tracking technology in manufacturing and logistics: Systematic literature review and research agenda. *Computers & Industrial Engineering*, 108444.