



**VILNIAUS UNIVERSITETO
VERSLO MOKYKLA**

SKAITMENINĖS RINKODAROS STUDIJŲ PROGRAMA

Fausta Šerytė

MAGISTRO BAIGIAMASIS DARBAS

PRIVATUMO POLITIKOS INFORMACIJOS PATEIKIMO FORMATŲ POVEIKIS VARTOTOJŲ APSISPRENDIMUI ĮSIDIEGTI MOBILIĄSIAS APLIKACIJAS	IMPACT OF PRIVACY POLICY INFORMATION PRESENTATION FORMATS ON CONSUMERS' DECISION TO INSTALL MOBILE APPLICATIONS
--	--

Studentas _____
(parašas)

Darbo vadovas _____
(parašas)

Lekt. Gintarė Gulevičiūtė

Darbo vadovo vardas, pavardė

Vilnius, 2021 m.

SANTRAUKA

VILNIAUS UNIVERSITETO
VERSLO MOKYKLA
SKAITMENINĖS RINKODAROS PROGRAMA
FAUSTA ŠERYTĖ
PRIVATUMO POLITIKOS INFORMACIJOS PATEIKIMO FORMATŲ POVEIKIS VARTOTOJŲ
APSISPRENDIMUI ĮSIDIEGTI MOBILIĄSIAS APLIKACIJAS

Darbo vadovas – lekt. Gintarė Gulevičiūtė
Darbas parengtas – 2021 m. Vilniuje
Darbo apimtis – 124 puslapiai.
Lentelių skaičius darbe – 17 vnt.
Paveikslų skaičius darbe – 7 vnt.
Literatūros ir šaltinių skaičius – 116 šaltinių

Pasauliniu mastu vis didėjantis mobiliųjų aplikacijų atsisuntimų skaičius kasmet auga. Todėl paraleliai auga ir mobiliųjų aplikacijų konkurencinė aplinka. Todėl pasitikėjimas aplikacijomis ir jų kūrėjais gali būti užtikrinamas teisingai įgyvendinant duomenų apsaugos praktikas. Visgi, duomenų apsauga ne visada yra realiai užtikrinama ar pateikiama vartotojams supaprastinta kalba.

Pagrindinis šio darbo tikslas yra nustatyti privatumo politikos informacijos pateikimo formatų poveikį ketinimui įsidiesti mobiliąsias aplikacijas esant skirtingoms jų kategorijoms. Darbas buvo suskirstytas į tris dalis.

Pirmoje darbo dalyje nagrinėjami privatumo politikos tikslai bei baziniai duomenų apsaugos reikalavimai, mobiliųjų aplikacijų kategorijos, suvokiama rizika ir pasitikėjimas, susijęs su duomenų apsauga, privatumo politikos informacijos komunikavimo ir vizualizavimo pagrindai, ketinimui įsidiesti aplikacijas turintys kintamieji. Antroje dalyje – aprašoma tyrimo metodika, iškeliamos hipotezės. Trečiojoje dalyje analizuojami kiekybinio tyrimo rezultatai, nustatoma, kokie privatumo politikos pateikimo formatai lemia vartotojų apsisprendimą įsidiesti mobiliąsias aplikacijas, pateikiamos išvados ir pasiūlymai.

Tyrime analizuojamos 2 skirtingos mobiliųjų aplikacijų kategorijos – socialinių tinklų ir kasdieninių finansų. Iš viso anketinėje internetinėje apklausoje dalyvavo 245 respondentai. Naudoti šie empirinių duomenų apdorojimo metodai: duomenų trianguliacija, faktorinė ANOVA, koreliacija, tiesinė regresija, moderacija. Tyrimui panaudotas 2x2x2 faktorinis dizainas (vizualus ir nevizualus privatumo politikos pranešimo pateikimas; utilitarinė ir hedoninė aplikacija; rizikinga ir nerizikinga aplikacija).

Rezultatai parodė, kad privatumo politikos pranešimo formatų svarbos vertinimas skiriasi nuo vizualinio pateikimo. Vizuali pateiktis teigiamai veikia požiūrį į aplikacijas ir ketinimą jas įsidiesti.

Taip pat suvokiama rizika ir suvokiamas pasitikėjimas skiriasi nuo skirtingos privatumo pranešimo rizikingumo pateikties. Rezultatai parodė, jog mobiliosios aplikacijos kategorija, respondentų

lytis bei amžius nebuvo svarbūs kintamieji tyrime. Darbe pateikiamas išvadas būtų galima pritaikyti rinkodaros tikslams, tolimesniems tyrimams bei verslui, plėtojančiam veiklą per mobiliąsias aplikacijas.

SUMMARY

VILNIUS UNIVERSITY
BUSINESS SCHOOL
DIGITAL MARKETING STUDY PROGRAMME
FAUSTA ŠERYTĖ
IMPACT OF PRIVACY POLICY INFORMATION PRESENTATION FORMATS ON
CONSUMERS' DECISION TO INSTALL MOBILE APPLICATIONS

Supervisor – lecturer Gintarė Gulevičiūtė

Paper prepared – 2021 in Vilnius

Paper scope – 124 pages

Number of tables – 17

Number of images – 7

Number of literature sources – 116 sources

Globally, the growing downloads of mobile applications is growing every year. As a result, the competitive environment for mobile applications is growing in parallel. Therefore, trust in applications and their developers can be ensured through the correct implementation of data protection practices. However, data protection is not always actually ensured or provided to consumers in a simplified language.

The main purpose of this work is to determine the impact of privacy policy information presentation formats on the intention to deploy mobile applications in different categories. The work was divided into three parts.

The first part examines the objectives of the privacy policy and the basic data protection requirements, the categories of mobile applications, the perceived risks and trust related to data protection, the basics of communication and visualization of privacy policy information, the variables to implement applications. In the second part - the research methodology is described, hypotheses are raised. The third part analyses the results of the quantitative study, identifies the formats of the presentation of the privacy policy that determine the consumers' decision to implement mobile applications, and presents the conclusions and suggestions.

The study analyses 2 different categories of mobile applications - social networking and everyday finance. A total of 245 respondents participated in the online questionnaire. The following empirical data processing methods were used: data triangulation, factor ANOVA, correlation, linear regression, moderation. A 2x2x2 factor design was used for the study (visual and non-visual presentation of the privacy policy statement; utilitarian and hedonic application; risky and non-risky application).

The results showed that the assessment of the importance of privacy policy message formats differs from the visual presentation. Visual presentation has a positive effect on the approach to

applications and the intention to implement them. Perceived risk and perceived trust also differ from the different risk presentation of a privacy statement. The results showed that the category of the mobile application, the gender and the age of the respondents were not important variables in the study. The conclusions presented in the work could be applied for marketing purposes, further research and business developing activities through mobile applications.

TURINYS

LENTELIŲ SĄRAŠAS	7
PAVEIKSLŲ SĄRAŠAS	8
ĮVADAS	9
1. PRIVATUMO POLITIKOS INFORMACIJOS PATEIKIMO FORMATŲ POVEIKIO VARTOTOJŲ APSISPRENDIMUI ĮSIDIEGTI MOBILIĄSIAS APLIKACIJAS TEORINIAI ASPEKTAI	12
1 . 1. Privatumo politikos tikslai ir duomenų apsaugos principai	12
1. 2. Mobiliųjų aplikacijų kategorijos ir jų vertės, leidimai, sukeliantys didžiausią vartotojų rizikos suvokimą	14
1. 3. Požiūrį į aplikacijas lemiantys veiksniai veikiantys ketinimą įsidiegti aplikacijas.....	16
1. 4. Vartotojų noras pateikti informaciją, privatumo politikos informacijos komunikavimo ir vizualizavimo įtaka, veikianti ketinimą įsidiegti aplikacijas	20
1. 5. Vartotojų ketinimą įsidiegti mobiliąsias aplikacijas aiškinantys modeliai	24
2. KETINIMO ĮSIDIEGTI APLIKACIJAS TYRIMO METODIKA	28
2. 1. Empirinio tyrimo tikslas, uždaviniai, modelis ir hipotezės.....	28
2. 2. Tyrimo metodai, instrumentai ir eiga.....	31
3. TYRIMO REZULTATŲ ANALIZĖ IR APTARIMAS.....	37
3. 1. Tyrimo rezultatų analizė	37
3. 2. Tyrimo hipotezių tikrinimas.....	39
3. 3. Pagrindinių situacijose naudotų manipuliacijos faktorių tarpusavio ryšių analizė	44
3. 4. Tyrimo ribotumai	48
IŠVADOS IR PASIŪLYMAI.....	50
LITERATŪROS IR ŠALTINIŲ SĄRAŠAS.....	53
PRIEDAI.....	64

LENTELIŲ SĄRAŠAS

1 lentelė. Anketoje naudoti konstruktai ir klausimai	33
2 lentelė. Ankstesnių tyrimų imties dydžio palyginimas	35
3 lentelė. Konstrukty patikimumo bei suderinamumo patikrinimas remiantis Cronbach alfa koeficientu	36
4 lentelė. Respondentų amžiaus ir lyties pasiskirstymas procentais skirtingose anketose, N=245 ..	37
5 lentelė. Vyrų ir moterų pasiskirstymas priskiriamai fundamentalistų kategorijai	38
6 lentelė. Vyrų ir moterų pasiskirstymas priskiriamai pragmatistų kategorijai	38
7 lentelė. Vyrų ir moterų pasiskirstymas nesusirūpinusių privatumu kategorijai.....	39
8 lentelė. Stjudento T-testo rezultatai lyginant vizualų ir nevizualų privatumo politikos pranešimų formatų įtaką suvokiamai vartotojų rizikai.....	40
9 lentelė. Stjudento T-testo rezultatai lyginant vizualų ir nevizualų privatumo politikos pranešimų formatų įtaką veikiančį suvokiamą pasitikėjimą	40
10 lentelė. Suvokiamo pasitikėjimo ir suvokiamos rizikos koreliacija	41
11 lentelė. Suvokiamo pasitikėjimo ir suvokiamos rizikos T- testo rezultatai	41
12 lentelė. Stjudento T-testo rezultatai lyginant vartotojų požiūrį į aplikaciją esant rizikingam ir nerizikingam privatumo pranešimui	42
13 lentelė. Požiūrio į aplikacijas ir ketinimo jas įsidiesti koreliacija.....	43
14 lentelė. Hipotezių rezultatai.....	44
15 lentelė. Faktorinė ANOVA vertinant privatumo politikos pranešimo formatų svarbą.....	45
16 lentelė. Faktorinė ANOVA vertinant suvokiamos rizikos svarbą	46
17 lentelė. Faktorinė ANOVA vertinant suvokiamo pasitikėjimo svarbą.....	47

PAVEIKSLŲ SĄRAŠAS

1 paveikslas.	<i>TAM modelio struktūra</i>	24
2 paveikslas.	<i>Planuotos elgsenos teoriją aiškinantis modelis</i>	25
3 paveikslas.	<i>C-HIP modelio struktūra.....</i>	26
4 paveikslas.	<i>Tyrimo modelis.....</i>	28
5 paveikslas.	<i>Aplikacijos tipo ir privatumo politikos nuostatų pateikimo iteracija.....</i>	46
6 paveikslas.	<i>Aplikacijos tipo ir privatumo pranešimo rizikingumo lygmens iteracija.....</i>	47
7 paveikslas.	<i>Aplikacijos tipo ir privatumo pranešimo rizikingumo lygmens iteracija.....</i>	48

IVADAS

„Statista“ (2019) duomenimis, nuo 2015 iki 2022 pastebimas ir prognozuojamas vis augantis išmaniųjų telefonų naudojimas Lietuvoje (Statista, 2019). Be to, analizuojant 2016 – 2019 metų „Google Play“ mobiliųjų aplikacijų parduotuvės duomenis, pastebimas bendras mobiliųjų aplikacijų parsisiuntimų skaičiaus vienetais augimas iki 84.3 mlrd. pasauliniu mastu (Statista, 2020). Didėjant bendram mobiliųjų aplikacijų parsisiuntimo skaičiui, lygiagrečiai auga aplikacijų kūrėjų konkurencinio pranašumo paieškos. Norint užtikrinti pasitikėjimą aplikacijomis, duomenų apsauga ir jos užtikrinimas tampa tai įrodančiu rodikliu. Tai ypač svarbu daugeliui verslų, kurie savo veiklą plėtoja per mobiliąsias aplikacijas. Pasak Chin, Felt, Sekar ir Wagner (2012), išmaniųjų įrenginių vartotojai, atsižvelgiant į duomenų apsaugos suvokimą, yra labiau susirūpinę išmaniojo telefono privatumo politikos ir duomenų apsaugos užtikrinimu lyginant su nešiojamais kompiuteriais. Ypač, kai mobiliųjų aplikacijų pagalba yra fiksuojamas ir perduodamas asmens atvaizdas, skenuojami biometriniai duomenys ar kitais būdais renkama jautrių asmens duomenų kategorijai priskiriama informacija. Todėl vartotojui, nesusidūrusiam su teisinėmis sąvokomis, privatumo politikos nuostatų išdėstymas bei įvairių leidimų tvarkyti asmens duomenis prašymas, gali sukelti tam tikrą suvokiamą riziką dėl savo duomenų apsaugos. Be to, ne visose šalyse yra vienodai suvokiama ir užtikrinama privatumo politika (Gu, Xu. C., Xu, Zhang ir Ling, 2016; Wang ir Lin, 2016), todėl moksliniuose tyrimuose yra pateikiami įvairiapusiai apibendrinimai ir išvados.

Anksčiau atliktuose tyrimuose, siejamuose su privatumo politika, nagrinėjamos: pasitikėjimo ir privatumo užtikrinimo tarpusavio sąveikos (Nikkhah, Balapour ir Sabherwal, 2018; Wu, Huang, Yen ir Popova, 2012); suvokiama privatumo politikos leidimų kontrolė (Chang, Wong, Libaque-Saenz ir Lee, 2018); privatumo politikos neapibrėžtumas (Aleem, Cavusoglu ir Benbasat, 2017); mobiliųjų aplikacijų sistemos, informacijos pateikimo ir paslaugų kokybės įtaka vartotojų suvokiamai privatumo politikos rizikai ir pasitikėjimui aplikacija (Wang ir Lin, 2016); privatumo politikos užtikrinimas ir informacijos nutekinimo grėsmės lyginant mobiliąsias aplikacijas ir internetinius tinklapius (Papadopoulos, E., Diamantaris, Papadopoulos, Petsas, Ioannidis ir Markatos, 2017); teisinis privatumo politikos suvokimas iš vartotojo perspektyvos (Strahilevitz ir Kugler, 2016); suvokiama mobiliųjų aplikacijų vertė prieš ketinant jas įsidiesti (Harris, Brookshire ir Chin, 2016) bei mobiliųjų aplikacijų parduotuvių prašomos prieigos prie vartotojų duomenų atskleidimo ypatumai (Gu ir kt., 2016).

Apsisprendimui įsidiesti ir naudotis mobiliosiomis aplikacijomis ypač svarbus supratimas, kaip vartotojai suvokia pateikiamą privatumo politikos informaciją (Chong, Ge, Li ir Proctor, 2018) ir ar įsitraukia į susipažinimą su nuostatais. Pasak Steinke (2002), nepasitikėjimas ir nerimas dėl asmens duomenų saugumo tampa kliūtimis el. komercijos vystymuisi. Išlieka neaišku, koks renkamų asmens duomenų bei privatumo politikos nuostatų informacijos pateikimo formatas leidžia sustiprinti vartotojų pasitikėjimą mobiliųjų aplikacijų saugumu, ypač jei yra renkami jautrūs duomenys. Bet koks netinkamas

duomenų atskleidimas gali sumažinti aplikacijų įsidieгимų skaičių, jei vartotojai yra ypač susirūpinę duomenų apsauga, ar yra nukentėję nuo netinkamo duomenų tvarkymo (Gu ir kt., 2016).

Anksčiau atliktuose tyrimuose buvo įtraukiami įvairūs skirtingi kintamieji, nagrinėjamos kultūriškai skirtingos šalys. Pasak Wu ir kt. (2012), privatumo politikos rizikos suvokimui ir susirūpinimui dėl jos įtakos turi kultūrinai skirtumai. Todėl galima teigti, jog lytis ir tiriamųjų amžius (Ismail, Ahmed, Kapadia ir Reiter, 2015) taip pat gali būti svarbūs. Tačiau Chang ir kt. (2018) bei Malik, Suresh ir Sharma (2017) teigia, kad rizikos dėl duomenų apsaugos supratimą veikia skirtinga mobiliųjų aplikacijų kategorija. Šiam teiginiui pritaria Jones, Sailaja ir Kerlin (2017), teigdami, kad vizualiniai sprendimai, padedantys supaprastinti privatumo politikos nuostatų supratimą bei didinantys išitraukimą, priklauso nuo mobiliosios aplikacijos funkcijų ar kategorijos. Chin, Harris ir Brookshire (2018) pateikia įžvalgas, jog suvokiama mobiliųjų aplikacijų nauda, ar net jų kūrėjo reputacija, gali turėti įtakos apsisprendimui įsidiegti aplikacijas. Be to, autoriai pabrėžia, kad tolimesniems tyrimams naudinga išsiaiškinti ar mobiliosios aplikacijos populiarumas keičia vartotojų požiūrį į duomenų apsaugą ir privatumo politiką (Zhang ir Xu, 2016). Kiti mokslininkai teigia, kad žinių spraga gali paveikti elgseną, susijusią su suvokiamu duomenų saugumu ir privatumu (Crossler ir Bélanger, 2017). Ne visuose tyrimuose buvo atsižvelgiama į tirtų šalių gyventojų technologinį raštingumą ar išsilavinimą. Technologinis raštingumas gali turėti įtakos bendram duomenų apsaugos supratimui ir elgesiui, priimant sprendimą pateikti savo duomenis. Taigi, atsižvelgus į skirtingų mokslininkų įžvalgas bei diskusijas, suvokiamą riziką dėl duomenų saugumo lemiantys veiksniai, prieš įsidiegiant mobiliąsias aplikacijas, gali būti skirtingi.

Empiriniuose tyrimuose vyrauja neapibrėžtumas, koks informacijos pateikimo formatas apie renkamus duomenis bei jų tvarkymą gali lemti vartotojų ketinimą įsidiegti mobiliąsias aplikacijas, jaučiantis saugiai dėl duomenų apsaugos. Pasak Flavián ir Guinalíu (2006), būsimuose tyrimuose naudinga tirti tokį veiksni, kaip galimybę kontroliuoti bei tvarkyti savo asmens duomenis, kurie gali paveikti suvokiamą riziką parsisiunčiant mobiliąsias aplikacijas. Galimos kontrolės kintamasis leistų identifikuoti vartotojo elgesį, kai mobiliosios aplikacijos reikalauja patvirtinti visus prieigos prie duomenų leidimus, norint visavertiškai naudotis aplikacija. Jones ir kt. (2017) pabrėžia, kad skirtinga aplikacijos kategorija nevienodai veikia vartotojų pasitikėjimą pateikiant jautrius duomenis, todėl tolimesniuose tyrimuose naudinga tirti privatumo politikos ir renkamų duomenų informacijos pateikimo formatus skirtingų aplikacijų kategorijų atžvilgiu. Atkreipiant dėmesį į tyrimo metodiką, keletas mokslininkų pabrėžia, jog tolimesniuose tyrimuose vertėtų panaudoti didesnio balo (7 - 10) Likerto skales tikslesniems rezultatams gauti (Chin ir kt., 2018; Harris ir kt., 2016).

Darbo problema – koks privatumo politikos informacijos pateikimo formatas gali lemti mažesnę vartotojų susirūpinimą jų privatumu, prieš ketinant įsidiegti mobiliąsias aplikacijas?

Darbo tikslas – nustatyti privatumo politikos informacijos pateikimo formatų poveikį ketinimui

įsidiegti mobiliąsias aplikacijas esant skirtingoms jų kategorijoms.

Darbo uždaviniai:

- 1) išanalizuoti privatumo politikos duomenų apsaugos aspektus, atitinkančius duomenų apsaugos direktyvą;
- 2) įvertinti mobiliųjų aplikacijų naudingumą bei vertes esant skirtingoms jų kategorijoms;
- 3) išanalizuoti suvokiamos rizikos ir pasitikėjimo įtaką ketinimui įsidiegti aplikacijas;
- 4) nustatyti privatumo politikos informacijos komunikavimo ir vizualizavimo pagrindus;
- 5) pateikti išvadas ir rekomendacijas apie privatumo politikos informacijos pateikimo formatų įtaką, lemiančią vartotojų apsisprendimą įsidiegti mobiliąsias aplikacijas.

Tyrimo metodai:

Darbo metodologija: Pasirinkta kiekybinė metodologija. Ji įgyvendinama šiais teoriniais ir empiriniais metodais:

Teoriniai metodai: dokumentų analizė, naratyvinė analizė.

Empirinių duomenų rinkimo metodai: internetinė anketinė apklausa.

Empirinių duomenų apdorojimo metodai: statistinis hipotezių tikrinimas, grafinis apdorojimas, duomenų trianguliacija, 2x2x2 faktorinis dizainas ir analizė, koreliacija, tiesinė regresija, moderacija.

Darbo struktūra: santrauka lietuvių bei anglų kalba, 3 turinio skyriai (pirmoje dalyje – remiantis moksliniais straipsniais ir kitais šaltiniais, nagrinėjami privatumo politikos tikslai bei baziniai duomenų apsaugos reikalavimai, mobiliųjų aplikacijų kategorijos, suvokiama rizika ir pasitikėjimas, susijęs su duomenų apsauga, privatumo politikos informacijos pateikimo formatai, ketinimui įsidiegti aplikacijas turintys veiksniai; antroje dalyje – aprašoma tyrimo metodika, iškeliamos hipotezės, vertinamas konstrukto patikimumas bei tyrimo eiga, trečiojoje dalyje, atlikus kiekybinį tyrimą, nustatoma, kokie privatumo politikos pateikimo formatai lemia vartotojų apsisprendimą įsidiegti mobiliąsias aplikacijas, nustatomi darbo ribotumai, pateikiamos tyrimo išvados bei pasiūlymai), įvadas, dėstymas, išvados ir rekomendacijos, literatūros ir šaltinių sąrašas, priedai. Darbo apimtis – 124 puslapiai.

1. PRIVATUMO POLITIKOS INFORMACIJOS PATEIKIMO FORMATŲ POVEIKIO VARTOTOJŲ APSISPRENDIMUI ĮSIDIEGTI MOBILIĄSIAS APLIKACIJAS TEORINIAI ASPEKTAI

1 . 1. Privatumo politikos tikslai ir duomenų apsaugos principai

Įskiepiami mobiliosiose aplikacijose leidžia sekti, stebėti, rinkti, analizuoti tam tikrus vartotojų veiksmus ar duomenis, kurie dažniausiai būna panaudojami rinkodaros, personalizuotos reklamos, užsakymų procesų vykdymo ir kitais tikslais. Privatumo politikos nuostatai leidžia vartotojams suprasti, kokie asmens duomenys yra renkami, perduodami, tvarkomi ir saugomi. Taip pat, duodami sutikimai tvarkyti asmens duomenis, apsaugo vartotojus nuo žmogaus teisių pažeidimo bei grubaus duomenų panaudojimo rinkodaros tikslais (Steinke, 2002). Asmens duomenys gali būti suprantami kaip bet kokia pateikiama informacija, leidžianti identifikuoti konkretų asmenį (Europos komisija). Tai gali būti asmens vardas bei pavardė, namų adresas, lokacija, pajamos, IP kodas, slapukų identifikatoriai, ligos istorija, asmeninis elektroninis paštas ir kiti asmens tapatybę ar būvimo vietą galintys nusakyti duomenys (Europos komisija).

Įgyvendinant privatumo politikos nuostatų pritaikymą mobiliosioms aplikacijoms, renkami ir apdorojami asmens duomenys yra tvarkomi pagal tam tikros šalies, kurioje yra vykdoma veikla, reglamentus. Plačiausiai pasaulyje yra žinomi JAV ir ES požiūrių skirtumai į privatumo politiką bei duomenų apsaugą. Lietuvoje veikiančioms įmonėms yra taikomas 2018 m. ES įsigaliojęs bendrasis duomenų apsaugos reglamentas (toliau darbe – BDAR).

BDAR skirtas išspręsti duomenų apsaugos ir internetinės privatumo teisės iššūkius (Limba, Driaunys, Kiškis ir Šidlauskas, 2020). Be to, BDAR užkerta kelia galimomis manipuliacijomis su vartotojų elgesio duomenimis, duomenų panaudojimu politiniais tikslais bei reguliuoja bendrą didelių duomenų kiekio saugumo užtikrinimą (European Parliament). Taip pat ES yra vadovaujasi Europos Sąjungos duomenų apsaugos direktyva, kuri užtikrina asmens duomenų saugumą kaip ir kitas žmogaus teises (Esteve, 2017). Mobiliųjų aplikacijų naudotojams privatumo politikos nuostatai bei jų laikymąsi turėtų būti tapatinamas su pasitikėjimu ir saugiu aplikacijų naudojimu (Martin ir Shilton, 2016). Todėl pateikiama privatumo politika vartotojams suteikia aiškumo, kodėl yra prašoma pateikti tam tikrus duomenis ar suteikti prieigas (Lin, Sadeh, Amini, Lindqvist, Hong ir Zhang, 2012). Tokiu būdu išvengiama interpretacijų, jog tam tikri leidimai bus panaudoti tiesioginės rinkodaros ar kitais tikslais. Todėl teisingas privatumo politikos nuostatų pateikimas mobiliosioms aplikacijoms yra būtinas, norint užtikrinti vartotojų duomenų saugumą bei pelnyti vartotojų pasitikėjimą aplikacija ar mobiliųjų aplikacijų parduotuve. Atliktose studijose teigiama, kad supaprastintas vartotojų informavimas apie duomenų tvarkymą, skatina vartotojus priimti pagrįstus sprendimus (Tsfay, Hofmann, Nakamura,

Kiyomoto ir Serna, 2018).

Teisėtumas, tikslo apribojimai, teisingumas ir skaidrumas, vientisumas ir konfidencialumas, duomenų minimizavimas, tikslumas, saugojimo apribojimai – sudaro pagrindinius BDAR duomenų apsaugos principus (Limba ir kt., 2020). Papildant ir išplėtojant šį teiginį, remiantis Steinke (2002), BDAR taikymas turi atitikti reikalavimus, tokius kaip:

1. Informavimas: vartotojai turi būti informuojami, kokių tikslų renkami duomenys, kaip susisiekti su įmone bei pateikti trečiųjų šalių tipus, kurioms atskleidžiama informacija;

2. Galimybė atsisakyti: vartotojams privalo būti suteikta teisė atsisakyti pateikti tam tikrus duomenis. Be to, vartotojams turi būti suteikiama teisė reikalauti ištrinti visus sukauptus duomenis (Tesfay ir kt., 2018);

3. Duomenų saugojimas: įmonių atsakomybė užtikrinti bei laikyti duomenų apsaugos. Nustatomas asmens duomenų saugojimo laikotarpis, atsižvelgiant į tikslus, kuriais remiantis įmonės saugo ir kaupia duomenis (Tesfay ir kt., 2018);

4. Prieiga prie informacijos: vartotojams turi būti suteikiama galimybė tvarkyti suteiktus leidimus bei turėti prieigą prie savo asmeninės informacijos.

Užtikrinus visus galimus reikalavimus, tikslus privatumo politikos taikymas gali būti panaudojamas kaip konkurencinis pranašumas (Gimpel, Kleindienst, Nüske, Rau ir Schmied, 2018). Mobilųjų aplikacijų valdytojams aiškus privatumo politikos pateikimas tampa ne tik pasitikėjimo, bet ir ryšio su vartotojais kūrimo įrankis (Bansal, Zahedi ir Gefen, 2015). Tokiu būdu kuriamas vartotojų pasitikėjimas, užtikrinant asmens duomenų saugumą, gali padidinti rinkos lojalumą (Flavián ir Guinalíu, 2006). Ermakova, Baumann, Fabian, ir Krasnova (2014) atliktame empiriniame tyrime pabrėžė, jog esamas pasitikėjimas internetinėmis platformomis, teigiamai veikia suvokimą perskaityti privatumo politikos nuostatus. Galima teigti, jog aiškus informacijos pateikimas gali paveikti vartotojų elgesį (Kelley, Cranor ir Sadeh, 2013). Teigiama, kad aiškus privatumo politikos nuostatų pateikimas mobiliosiose aplikacijose turi įtakos ketinimui jas įsidiegti (Kununka, Mehandjiev ir Sampaio, 2018; Steinke, 2002).

Taigi, privatumo politikos įstatymai leidžia apsaugoti vartotojus nuo duomenų nutekimo, organizacijų grubių asmens duomenų pažeidimų bei grubių rinkodarinių tikslų įgyvendinimo. BDAR siekiama įvesti kiek įmanoma daugiau aiškumo ir skaidrumo duomenų valdymo ir teisės atžvilgiu. Užtikrinant asmens duomenų apsaugą, vartotojai, besinaudojantys internetinėmis platformomis ar mobiliosiomis aplikacijomis, jaučiasi saugesni, informuoti bei gali tapti labiau lojalūs. Vartotojams suteikiamas pakankamas informuotumas bei skaidrumas apie galimas grėsmes, sumažina aplikacijos rizikingumą bei stiprina vartotojų pasitikėjimą. Šio darbo tyrimo analizei bus naudojamas skirtingas privatumo politikos pateikimo būdas, remiantis baziniais BDAR reikalavimais.

1. 2. Mobiliųjų aplikacijų kategorijos ir jų vertės, leidimai, sukeliantys didžiausią vartotojų rizikos suvokimą

Prieš ketinant įsidiegti mobiliąsias aplikacijas, vartotojai turi susidaryti tam tikrus lūkesčius bei suvokimą, kokie duomenys gali būti renkami, atsižvelgiant į mobiliosios aplikacijos kategoriją (Lin ir kt., 2012). Remiantis Flora, Wang ir Chande (2014), išskiriamos šios mobiliųjų aplikacijų kategorijos: komunikacijos, žaidimų, multimedijų, kelionių, edukacinės, produktyvumo, paslaugų. Bansal, Zahedi ir Gefen (2008) atlikto tyrimo apie asmens duomenų pateikimą ir pasitikėjimą rezultatuose teigiama, kad privatumo politikos duomenų aiškumas, atsižvelgiant į mobiliosios aplikacijos kategoriją, yra ypač svarbus ketinimui pateikti savo duomenis ir kurti pasitikėjimą aplikacijos valdytoju. Tai ypač svarbu, kai rinkoje egzistuoja nemažai panašaus tipo mobiliųjų aplikacijų, kurios gali būti įsidiegiamos iš skirtingų aplikacijų kūrėjų/valdytojų. Panašios nuomonės laikosi ir kiti autoriai, teigdami, jog asmens duomenų valdymo reikšmė ir noras apsaugoti savo duomenis priklauso nuo mobiliosios aplikacijos ar internetinės platformos reikšmės tiek vartotojui, tiek aplikacijos ar platformos tikslams pasiekti (Aïmeur, Lawani ir Dalkir, 2016). Krafft, Arden ir Verhoef (2017) kartu su Aïmeur ir kt. (2016) teigia, kad suvokiama organizacijos produkto vertė vartotojui yra stimulus pasitikėti aplikacija ir leisti suteikti prieigą prie duomenų. Pasak Kerviler, Demoulin ir Zidda (2016), suvokiamas vertės, susijusias su rizikos suvokimu, galima skirstyti į hedonines, utilitarines, socialines ir epistemines (Wang, Liao ir Yang, 2013). Hedoninės vertės siejamos su vartotojų džiaugsmu, pramogomis, patyrimais. Utilitarinės vertės siejamos su finansine nauda, patogumu, informacijos pakankamumu (Kerviler ir kt., 2016). Socialinės naudos gali būti siejamos su socialinėmis grupėmis, noru kurti savo įvaizdį kitų akyse. Socialinės vertės naudojant mobiliąsias aplikacijas pasireiškia socialinės gerovės gerinimu (Wang ir kt. 2013). Epistemologinės vertės skatina norą pažinti bei sužinoti. Mobiliųjų aplikacijų kontekste, tai noras išbandyti naują paslaugą ar technologiją (Wang ir kt. 2013). Asmens suvokiamas aplikacijos naudingumas didina tikimybę suteikti prieigą asmens duomenų tvarkymui (Krafft ir kt., 2017; Tay, Teh ir Payne, 2021). Tačiau, remiantis Kerviler ir kt. (2016), suvokiama rizika yra svarbesnė nei utilitarinės, hedoninės ar socialinės naudos. Autoriai Hur, Lee ir Choo (2017) empirinio tyrimo apie mobiliųjų aplikacijų paslaugų naudojimosi ketinimus išvadose teigia, kad aplikacijos žaismingumas, suvokiamas naudingumas ir suvokiamas paprastumas naudojantis aplikacija padeda apsisprendimui jas įsidiegti. Pabrėžiama, kad suvokiamas aplikacijos naudingumas bei žaismingumas yra pirminiai medijuojantys veiksniai, skatinantys ketinimą naudotis aplikacijomis. Tačiau pabrėžiama, kad rezultatai gali skirtis nuo vartotojų amžiaus bei technologinio raštingumo. Krafft ir kt. (2017) empirinio tyrimo išvadose išskiriama, jog suvokiamas suteikiamas aplikacijos pramogų lygis teigiamai veikia ketinimą leisti valdyti asmens duomenis.

Aplikacijos, skirtos patenkinti skirtingus vartotojų poreikius, atitinkamai turi skirtingą reikšmę

susirūpinimui dėl privatumo ir galimų rizikų. Susirūpinimo privatumu skirtumai priklauso nuo aplikacijos kategorijos (Bergström, 2015). Finansinių, sveikatos, edukacijos reikmėms patenkinti skirtos aplikacijos gali būti suvokiamos kaip aukštesnės rizikos aplikacijos, kurios gali turėti įtaką asmeninei, psichologinei ar finansinei padėčiai. Remiantis Reuter, Häusser, Bien ir Herbert (2019) tyrimo rezultatais, vartotojai mobiliosios bankininkystės aplikacijas išskyrė kaip labiausiai duomenų apsaugos reikalaujančias aplikacijas. Bendrąja prasme vartotojai nesupranta, kaip jų pateikti asmeniniai duomenys bus naudojami, vartotojai nerimauja dėl savo privatumo ir finansinės informacijos naudojantis mobiliąja bankininkyste (Zhang, Lu ir Kizildag, 2018). Jei informacija laikoma tikslia, svarbia, laiku ir lengvai pateikiama, ji gali pagerinti vartotojų supratimą apie mobiliosios bankininkystės vertinimą (požiūrį) (Sreejesh, Anusree ir Mitra, 2016). Tyrimų rezultatuose teigiama, kad sistemiškai pateikiama informacija teigiamai veikia vartotojų ketinimą naudotis mobiliąja bankininkyste, taip pat vartotojams turi būti lengvai suprantama, kad mobiliosios bankininkystės valdytojai užtikrins saugumą bei apsaugos nuo apgaulės (Sreejesh ir kt., 2016). Zhang ir kt. (2018) tyrime teigiama, kad pagrindinės priežastys, kodėl vartotojai vengia naudotis mobiliąja bankininkyste yra susirūpinimas saugumu ir privatumu, neįžvelgiama nauda vartotojui. Todėl pastarieji tyrėjai teigia, jog yra naudinga tirti veiksnius, turinčius įtakos vartotojams naudotis mobiliosios bankininkystės paslaugomis.

Kitą vertus, pramoginio turinio aplikacijos gali sudaryti žemesnį suvokiamos rizikos lygį, nes pateikiami duomenys gali būti nuasmeninti, ar turėti tik leidimą analizuoti vartotojų veiksmus ir panaudoti juos personalizuotai reklamai ar pakartotinei rinkodarai. Be to, pramoginio turinio aplikacijos prašo mažiau riziką sukeliančių leidimų lyginant su utilitarinių reikmių aplikacijomis (Harris ir Chin, 2016). Tačiau Haggag (O), Haggag, Grundy ir Abdelrazek (2021) teigia priešingai, jog socialinių tinklų aplikacijos turi aiškias privatumo bei etikos problemas, surinkta informacija apie vartotojus galima panaudoti manipuliacijoms, išplėstinei vartotojų profilio analizei. Be to, patys vartotojai jaučia susirūpinimą dėl galimų rizikų susijusių su jų duomenimis socialiniuose tinkluose. Vartotojai tampa susirūpinę, jog kiti asmenys gali paviešinti jų asmeninius duomenis, pasinaudoti jų intelektine nuosavybe. Kitiems vartotojams privatumo nustatymai nėra iki galo aiškūs, vartotojai nesupranta kaip techniškai juos galėtų pritaikyti savo saugumui, taip pat pasitaiko, jog vartotojai yra linkę bet koku atveju nepasitikėti socialinių tinklų saugumu (Aïmeur, Gambs ir Ho, 2009). Tyrimuose teigiama, kad suvokimas ir pojūtis, jog duomenys yra saugūs, veikia bendrą vartotojų įsitraukimą į socialinius tinklus (Choi ir Sung, 2018).

Rizikos suvokimą ir susirūpinimą privatumu gali veikti ne tik aplikacijos kategorija. Įtakos gali turėti pertekliniai ar neaiškūs prašomi patvirtinti leidimai. Autoriai Harris ir Chin (2016) išskiria tokius dažniausiai pasikartojančius aukšto rizikingumo leidimus kaip: apytikslė lokacija, paskirų radimas ir naudojimas įrenginyje, USB rakto duomenų modifikacija arba naikinimas, tikslios lokacijos nustatymas, įrenginio būsenos ir tapatybės nuskaitymas, kalendoriaus ir konfidencialios informacijos nuskaitymas,

kontaktinės informacijos nuskaitymas, garso įrašinėjimas, nuotraukų darymas, teksto pranešimų nuskaitymas ir kiti. Atliktose studijose pabrėžiama, kad ryšys tarp mobiliųjų aplikacijų veiksmų bei jų vertinimo iš vartotojo perspektyvos, skiriasi (Hatamian, Serna ir Rannenberg, 2019). Todėl pateikiami leidimai vartotojams turėtų būti aiškiai suvokiami, kad suvokiama rizika duomenų saugumu nebūtų didesnė nei suvokiamas aplikacijos naudingumas.

Taigi, ketinimui įsidiesti mobiliąsias aplikacijas įtakos turi vartotojų suvokiamas aplikacijų naudingumas. Tyrimuose daugiausiai duomenų apsaugos reikalaujančiomis aplikacijos išskiriamos mobiliosios bankininkystės aplikacijos. Prieštaringos nuomonės laikomasi tiriant hedoninės, dažniausiai socialinių tinklų ar pramogines aplikacijas. Autorių nuomone, jos įvardijamos kaip žemesnės rizikos aplikacijos. Tačiau skirtingi tyrėjai socialinių tinklų programėles įvardija kaip daugiausia privatumo pažeidimų sukeliančias aplikacijas. Suvokiamas aplikacijų naudingumas siejamas su galimomis rizikomis ir požiūriu į jas. Aplikacijų rizikos suvokimą taip pat gali paveikti įvairūs prašomi suteikti leidimai. Viena iš labiausiai riziką sukeliančių leidimų laikomas apytikslės arba konkrečios lokacijos leidimas. Šio darbo tyrime anketose pateikiamoms situacijoms bus naudojamas lokacijos leidimas, tiriamos utilitarinės ir hedoninės aplikacijos (socialinių tinklų ir kasdieninių finansų).

1. 3. Požiūrį į aplikacijas lemiantys veiksniai veikiantys ketinimą įsidiesti aplikacijas

Mobiliosios aplikacijos yra priemonės prekės ženklų ir vartotojų tarpusavio komunikacijai (Kim, Yoon ir Han, 2014). Mobiliųjų aplikacijų parduotuvėse galima rasti nemažai konkurentų sukurtų aplikacijų, todėl svarbu suprasti veiksnius, kurie gali skatinti, arba atvirkščiai, neskatinti įsidiesti mobiliąsias aplikacijas.

Ankstesniuose tyrimuose pasitikėjimas (Harris ir kt., 2016; Chin ir kt., 2018; Harris, Chin ir Brookshire, 2015b), suvokiama rizika ir saugumas (Harris ir kt., 2016; Fong, Lam ir Law, 2017; Kerviler ir kt., 2016; Lai, Hsu ir Wu, 2018), suvokiama vertė (Harris ir kt., 2016; Vasconcelos, Barcellos, Viterbo, Bernardini, Boscarioli ir Nunes, 2019) ir mobiliųjų aplikacijų reitingo bei jų parduotuvių pasitikėjimas (Harris, Brookshire, Patten ir Regan, 2015a; Siegfried, Koch ir Benlian, 2015) įvardijami kaip apsisprendimui įsidiesti mobiliąsias aplikacijas turintys veiksniai. Be to, ketinimui naudotis aplikacijomis įtakos turi suvokiamas informatyvumas ir naudingumas, pramoginis turinys, socialinis naudingumas, ekonomiškumas bei vartotojų apžvalga (Kim ir kt., 2014). Visi šie veiksniai tarpusavyje skirtingai veikia vartotojų sprendimą aplikacijų įdiegimui.

Vartotojai, besinaudojantys internetinėmis paslaugomis, tikisi, kad jų pateikti asmens duomenys bus saugūs. Dažniausiai, prieš perskaitant ar ketinant skaityti privatumo politikos nuostatus, vartotojai turi susidaryti tam tikrą pasitikėjimo, saugumo ir rizikos suvokimą. Pasak Harris ir kt. (2016) tyrimo

rezultatų, suvokiamas saugumas, veikiantis suvokiamą riziką daro neigiamą įtaką ketinimui įsidiesti mobiliąsias aplikacijas. Tačiau autoriai pabrėžia, kad pasitikėjimas turi didelę teigiamą įtaką ketinimui jas įsidiesti. Be to, suvokiama rizika neturi stipraus ryšio, veikiančio vartotojų pasitikėjimą (Chin ir kt., 2018) kaip ir esantis žemas privatumo lygis mažina suvokiamą riziką (Lai ir kt., 2018). Bansal ir kt. (2015) išskiria vartotojus į žemo ir aukšto susirūpinimo savo asmens duomenimis kategorijas. Aukštą susirūpinimo duomenų saugumu lygį turintys vartotojai gali keisti savo požiūrį, jeigu bus kuriamas naudą vartotojui atitinkantis rinkodarinis turinys (Aïmeur ir kt., 2016). Be to, aukštą susirūpinimo kategoriją turintys asmenys dažnai susitelkia į asmens duomenų saugumo prevencijos veiksmus (Lwin, Wirtz ir Stanaland, 2016). Tokiu atveju vartotojai tikslingai vengia jų įsitikinimu dėl duomenų saugumo neatitinkančių organizacijų, ieško kitų alternatyvų. Kai kuriuose su duomenų apsauga susijusiuose tyrimuose buvo naudojamas A. Westin privatumo indekso nustatymas (Betzing, Tietz, Brocke ir Becker, 2019; Felt, Ha, Egelman, Haney, Chin ir Wagner, 2012). Šis indeksas vertina vartotojų požiūrį ir susirūpinimą privatumu (Kumaraguru ir Cranor, 2005). Remiantis Kumaraguru ir Cranor (2005), tyrėjas A. Westin vartotojus skirsto į 3 kategorijas:

1. Fundamentalistus: vartotojus, kurie turi itin aukštą susirūpinimo duomenų apsaugą lygį, linkę neatskleisti savo duomenų;
2. Pragmatistus: vartotojus, kuriems yra svarbi galimybė nuspręsti, ar jie nori atskleisti savo asmeninius duomenis;
3. Nesusirūpinusius privatumu: vartotojus, kurie pasitiki įmonėmis, per daug neanalizuodami situacijos pateikia savo duomenis.

Šios kategorijos nulemia suvokiamą riziką pateikiant asmeninius duomenis bei nusako, kaip turi keistis komunikacija su vartotojais, ir koks privatumo politikos duomenų pateikimo formatas turi būti aiškiausias ir įtikinantis. Komunikacijai apie galimas rizikas taip pat pasitelkiama vaizduoti privatumo rizikingumo lygmenis. Kadangi vartotojai linkę skirtingai vertinti ir įžvelgti rizikas, grafinis rizikingumo vaizdavimas ne tik padeda komunikuoti apie galimas grėsmes, bet ir padeda jas įvertinti (Chen, Ge, Moore, Yang, Li ir Proctor, 2018). Taip pat rizikos vaizdavimas padeda taupyti laiką rizikos vertinimui (Chen ir kt., 2018). Kai kuriuose tyrimuose grafinis privatumo rizikos lygmens vaizdavimas buvo labiau įvertintas ir pastebėtas vartotojų nei bendras aplikacijos reitingas (Gates, Chen, Li ir Proctor, 2014). Taip pat pastebėta, kad galimos rizikos įvertinimo svarba padidėja, kai ją vaizduojančios ikonos yra pateikiamos.

Punyatoya (2018) atliktame tyrime išskiria emocinį ir kognityvinį pasitikėjimą, darantį įtaką vartotojų elgesiui internete. Vartotojai, turintys didelį susirūpinimą dėl privatumo, yra linkę perskaityti, kognityviai apdoroti ir apsvarstyti privatumo informaciją (Choi ir Land, 2016). Priešingai, kai vartotojai yra mažiau susirūpinę dėl privatumo, tampa mažiau įsitraukę į vertinimą (Choi ir Land, 2016). Tyrimais nustatyta, kad didesnis vartotojų suvokiamas saugumas tvarkant jų asmens duomenis teigiamai veikia

suvokimą pasitikėjimą el. platformomis (Flavián ir Guinalíu, 2006). Norint formuoti vartotojų pasitikėjimą mobiliosiomis aplikacijomis, Bansal ir kt. (2015) atliktame empiriniame tyrime išskyrė šiuos faktorius: įmonės reputaciją, kuri siejama su didesne kokybe, informacijos ir grafikos kokybe, pakankamą informaciją apie įmonę. Atlikto tyrimo rezultatuose labiausiai išryškinama reputacijos, informacijos apie įmonę svarba ir bendra pateiktos informacijos kokybė. Aplikacijų kokybės suvokimui įtakos turi programėlių pardavėjo ar aplikacijų parduotuvės reputacija (Koch ir Benlian, 2015). Tai priklauso nuo bendro vartotojų požiūrio į aplikacijų parduotuvės kokybę, suvokiamą patikimumą ir asmeninę naudą. Be to, anot mokslininkų Harris ir kt. (2016) tyrimo rezultatų, suvokiama mobiliosios aplikacijos reputacija teigiamai veikia vartotojų pasitikėjimą, tačiau turi neigiamos įtakos suvokiamai rizikai. Teigiama, kad aiškiai suformuluotas bei adekvatus privatumo politikos teiginių pateikimas veikia vartotojų pasitikėjimą bei sumažina susirūpinimą duomenų saugumu (Bansal ir kt., 2015). Autoriai pabrėžia, kad šį ryšį moderuoja vartotojų susirūpinimas privatumu. Įmonės reputacija taip pat veikia vartotojų pasitikėjimą ir šis ryšys yra moderuojamas vartotojų susirūpinimu privatumu (Bansal ir kt., 2015). Panašios išvados gautos ir kitose empirinėse studijose, teigiančiose, kad reputacijos (Ruchi ir Kumar, 2018) ir komunikacijos (pateikiamos informacijos) su vartotojais kokybė teigiamai veikia ir pasitikėjimą, ir vartotojų rūpestį dėl jų privatumo (Lwin ir kt., 2016). Aplikacijų pardavėjo ar parduotuvės reputacija bei asmeninis vartotojų pasitikėjimas, saugumo kaip vertybės suvokimas gali būti skirtingai veikiamas vizualizacinių mobiliųjų aplikacijų sprendimų pateikimu. Yan, Liu, Niemi, ir Yu (2013) atlikto tyrimo duomenimis, pasitikėjimą ir reputaciją pabrėžiantys vizualizaciniai aplikacijų sprendimai dažniausiai keičia vartotojų elgseną bei padeda priimti sprendimus naudotis ar nesinaudoti aplikacija. Autoriai teigia, kad vartotojai labiau linkę tikrinti informaciją apie pačią mobiliąją aplikaciją ar jos kūrėjus, jei vartotojai turi stipriau išreikštą duomenų ar asmens saugumo siekį kaip vertybę. Todėl vizualizaciniai sprendimai, pabrėžiantys, kaip yra užtikrinamas asmens duomenų saugumas lemia didesnę vartotojų susidomėjimą ir ketinimą naudotis aplikacijomis.

Nors suvokiama įmonės reputacija ir pateiktos informacijos kokybė yra svarbi kuriant vartotojų pasitikėjimą, kitų autorių tyrimo išvadose teigiama, kad suteikiama kontrolė turi stipresnę teigiamą ryšį vartotojams, besirūpinantiems savo pateiktų asmens duomenų saugumu (Zhou, 2017; Martin, Borah ir Palmatier, 2017; Flavián ir Guinalíu, 2006; Aïmeur ir kt., 2016; Krafft ir kt., 2017). Vartotojui suteikiama kontrolė nebūtinai turi reikšti visišką duomenų kontrolę. Tai gali būti suvokiama duomenų kontrolė, kuri gali skatinti pasitikėjimą savo duomenų saugumu ir ketinimu pateikti asmens duomenis ar duoti prieigą prie jų (Martin ir kt., 2017). Galimybė kontroliuoti savo duomenis, dažnu atveju apsaugo asmenis nuo jautrių duomenų panaudojimo pažeidimų, sumažina suvokiamą duomenų apsaugos riziką. Aïmeur ir kt. (2016) atliktame tyrime, kuriame buvo siekiama suprasti ryšį tarp privatumo politikos pateikimo formatų ir vartotojų pasitikėjimo, teigiama, kad suteikiama duomenų kontrolė vartotojams yra vienas iš svarbiausių veiksnių naudojantis platformomis. Tai vartotojams

suteikia aiškumo ir jiems nereikia apsvarstyti alternatyvų (kitų platformų, mobiliųjų aplikacijų).

Kitose studijose suteikiama kontrolė nėra įvardijamas kaip tam tikrą įtaką pasitikėjimui duomenų saugumu turintis veiksnys. Papildomas aplikacijų vertes suvokti ir įvertinti padeda aplikacijų charakteristikos. Viena iš jų – reitingavimas. Reitingavimas siejamas su tam tikra kokybe, nes yra suvokiama, jog produktas, šiuo atveju aplikacija, buvo išbandyta. Be to, didesni nei vidutiniai įvertinimo rodikliai bei matytos reklamos apie aplikacijas teigiamai veikia suvokiamą aplikacijos kokybę, kuri paskatina įsidiegti aplikacijas (Siegfried ir kt., 2015; Chen, Gates, Li ir Proctor, 2015). Galima teigti, kad vartotojai dažnu atveju atkreips dėmesį į aplikacijos parsisiuntimų skaičių, atsiliepiamus, aplikacijų peržiūrų skaičius. Pasak Hammouri, Almajali, Nusairat ir Saraireh (2020) tyrimo rezultatų, pateikiamos rekomendacijos bei pasidalinta patirtis veikia būsimų vartotojų pasitenkinimą, o tai padeda priimant sprendimą įsidiegti aplikacijas. Parsisiuntimų skaičius taip pat gali būti suvokiamas kaip populiaros aplikacijos indikatorius (Ali, Joorabchi ir Mesbah, 2017). Kituose tyrimuose pastebima, kad vartotojai labiau linkę įsidiegti populiarias mobiliąsias aplikacijas nei nišines (Zhong ir Michahelles, 2013). Panašūs rezultatai gauti Gu ir kt. (2016) atliktame tyrime apie susirūpinimą duomenų saugumu prieš įsidiegtiant mobiliąsias aplikacijas. Rezultatuose teigiama, kad vartotojų suvokiamas aplikacijos populiarumas sumažina susirūpinimą asmens duomenų saugumu. Be to, vartotojų suvokiamą vertę gali stiprinti vartotojų įsitraukimas į patį pirkimo ar aplikacijos paieškos procesą. Kuo daugiau vartotojas susipažins su alternatyvomis, naudingumu ir kitų asmenų apžvalgomis, tuo labiau įgautos žinios padės apsispręsti, kurios aplikacijos labiausiai patenkintų vartotojų norus. Chong ir kt. (2018) tyrimo rezultatuose pastebima, kad įvardijamas ir esantis aukštesnis nei vidutinis mobiliosios aplikacijos saugumo ir vartotojų atsiliepiamų reitingas, didina vartotojų ketinimą įsidiegti aplikacijas.

Visus šiuos veiksnius ir jų ryšius moderuoja skirtingas vartotojų amžius bei lytis. Pasak Faqih (2016), lytis moderuoja ryšį tarp ketinimui įsidiegti aplikacijas turinčių veiksmų (pasitikėjimo, suvokiamos rizikos, naudojimosi patogumo, privatumo) ir vartotojų elgsenos (ketinimo). Lytis laikoma svarbiu moderuojančiu kintamuoju nagrinėjant vartotojų ketinimus įsidiegti aplikacijas (Hossain, 2019). Tačiau kiti tyrėjai teigia priešingai, jog lytis bendrąja prasme neturi įtakos susirūpinimui privatumu (Dimodugno, Hallman, Plaisent ir Bernard, 2021). Dėl vyraujančių tyrėjų nesutarimų lyties atžvilgiu, lyties skirtumus nagrinėti yra naudinga. Empirinių tyrimų rezultatuose amžius įvardijamas kaip įtakos privatumo susirūpinimui turintis kintamasis (Dimodugno ir kt., 2021). Vyresnio amžiaus vartotojams suvokiama aplikacijos vertė yra mažiau svarbi lyginant su privatumo svarba (Wottrich, Reijmersdal ir Smit, 2018). Taip pat vyresnio amžiaus vartotojai ženkliai skiriasi privatumo klausimų ir duomenų apsaugos supratimu, aktyviau nei jaunesni vartotojai saugo savo duomenis (Dimodugno ir kt., 2021). Galima teigti, kad skirtinga lytis bei amžius gali veikti vartotojų elgesį svarstant įsidiegti aplikacijas.

Mokslinėje literatūroje taip pat galima išvelti kitus svarbius veiksnius, turinčius įtakos apsisprendimui įsidiegti mobiliąsias aplikacijas, tokius kaip: vidinė kontrolė (Fong ir kt., 2017) ir patirtis

(Kerviler ir kt., 2016; Harris ir kt., 2015b), artimųjų ir pažįstamų asmenų rekomendacijos (Koch ir Benlian, 2015), finansiniai ar bonusiniai paskatinimai, registracijos mokestis (Krafft ir kt., 2017).

Taigi, bendrą požiūrį į aplikacijas lemia daugelis veiksnių. Dažniausiai jie susiję su rizikos ir pasitikėjimo faktoriais, elgesio bei vertės motyvais. Visi šie veiksniai yra tarpusavyje susiję ir gali daryti tiek teigiamą, tiek neigiamą įtaką vartotojų suvokimui dėl duomenų saugumo ir aplikacijos naudos. Susirūpinimas asmens duomenų saugumu prieš įsidiegiant mobiliąsias aplikacijas skiriasi nuo vartotojų susirūpinimo lygmens. Stiprinant pasitikėjimą aplikacijų saugumu, tam įtakos turi keletas veiksnių. Atliktose empirinėse studijose, didžiausią poveikį asmens duomenų rizikos suvokimui ir pasitikėjimui įtakos turi mobiliosios aplikacijos populiarumas bei kūrėjo reputacija, suteikiama duomenų kontrolė, aplikacijos naudingumas ir teisingas bei aiškus informacijos pateikimas. Visi šie veiksniai padeda suvoki galimas rizikas ir sukuria pasitikėjimą, kas lemia požiūrį į aplikacijas. Šio darbo tyrimo anketose pateikiamoms situacijoms bus naudojamas kontrolės faktorius, rizikos reitingas. Naudojamas Westin indeksas, siekiant įvertinti vartotojų požiūrį ir susirūpinimą privatumu.

1. 4. Vartotojų noras pateikti informaciją, privatumo politikos informacijos komunikavimo ir vizualizavimo įtaka, veikianti ketinimą įsidiegti aplikacijas

Prieš įsidiegiant mobiliąsias aplikacijas, svarbu suprasti, kaip vartotojai supranta pateiktą privatumo politikos kalbą, koks pateikimo būdas padeda ją teisingai ir aiškiai suprasti bei į kokius faktorius vartotojai atkreipia didžiausią dėmesį. Šis aiškus vartotojų supratimo apie informacijos, susijusios su privatumo politika, pateikimas mobiliųjų aplikacijų kūrėjams bei valdytojams leidžia tinkamai supažindinti vartotojus su jų duomenų apdorojimu bei saugojimu bei skatina neatmesti ketinimo įsidiegti aplikacijas dėl to, jog vartotojas jaučia galimas rizikas duomenų saugumu. Be to, svarbu suvokti, kokios privatumo politikos pateikimo savybės sumažintų suvokiamas rizikas ir didintų pasitikėjimą.

Prieš priimant sprendimą įsidiegti aplikacijas, vartotojams pateiktos privatumo politikos kalbos gali būti pateiktos per paprastai arba per sudėtingai (Zhao, Binns, Kleek ir Shadbolt, 2016), o jų privatumo lygio supratimas ir pateikimas taip pat gali būti skirtingas (Meinert, Peterson, Criswell ir Crossland, 2006). Teigiama, kad vartotojai labiau atkreipia dėmesį į aiškiai aprašytus privatumo politikos nuostatus nei į minimaliai ar visai nepateiktus nuostatus (Meinert ir kt., 2006). Šiam teiginiui taip pat pritaria Tsai, Egelman, Cranor ir Acquisti (2011), teigdami, kad vartotojai linkę teigiamai vertinti pateiktą privatumo informaciją nei visai nepateiktą, taip pat vartotojai atlieka daugiau konversijų, kai privatumo informacijos ikonos yra pateiktos. Tyrimų rezultatuose teigiama, kad pateiktos privatumo lygmenį vaizduojančios ikonos yra efektyvios priemonės komunikuojant informaciją apie privatumą (Tsai ir kt., 2011). Vaizduojamos aplikacijos duomenų ir privatumo rizika

indikuojančios ikonos turi reikšmingą įtaką aplikacijos pasirinkimui (Rajivan ir Camp, 2016), kurios gali būti efektyvesnės už vaizduojamą aplikacijos reitingą. Tyrimuose pabrėžiama, kad privatumo rizika indikuojantis ženklėjimas turi būti pateikiamas prieš svarstant įdiegti aplikacijas, turi sutapti su kitais aplikacijų charakteristikomis vaizduojančiais ženklėjimais, taip pat skirtingą rizikingumo lygmenį vaizduojančios ikonos turi būti patikimos ir susijusios su privatumo nuostatais (Rajivan ir Camp, 2016).

Meinert ir kt., (2006) atliktame empiriniame tyrime teigiama, kad noras pateikti asmens duomenis, skiriasi nuo jų tipo. Autorių atliktame tyrime, kuriame buvo tiriamas noras pateikti biografinius, finansinius ir kontaktinius duomenis, rezultatuose pastebima, kad vartotojai labiau linkę pateikti kontaktinę informaciją nei biografinę. Taip pat buvo pastebėta, jog vartotojams priimtinau pateikti biografinę informaciją nei finansinę informaciją (Meinert ir kt., 2006). Rezultatai leidžia identifikuoti, kad vartotojai prioritetuoja asmeninę informaciją, identifikuoja galimas aukštesnes ar žemesnes grėsmes, atsižvelgiant į informacijos tipą.

Vartotojų suvokimas, kad jų asmens duomenimis yra rūpinamasi, skatina ketinimą įsidiesti mobiliąsias aplikacijas (Balapour, Nikkhah ir Sabherwal, 2020; Martin ir Murphy, 2016). Vartotojų pasitikėjimas atsiranda tik tada, kai pateiktos privatumo politikos nuostatai yra realiai užtikrinami ir įgyvendinami (Meinert ir kt., 2006). Shklovski, Mainwaring, Skúladóttir ir Borgthorsson (2014) tyrimo rezultatuose teigiama, kad vartotojai jautėsi apgauti, kai jų suvokimas apie aplikacijoje renkamus duomenis ir leidimus skyrėsi nuo to, kokių leidimų buvo realiai prašoma.

Privatumo politikos nuostatomis išdėstyti yra pasirenkami skirtingi jų pateikimo būdai. Plačiausiai naudojamas būdas – tekstinis išdėstymas. Tai savotiškai komplikotas būdas išdėstyti tokio tipo informaciją, kai ne visi vartotojai gali vienodai suprasti teisinę kalbą, ar jų elgesys duomenų saugumo atžvilgiu gali būti žemas. Jones ir kt. (2017) empirinio tyrimo rezultatuose pastebima, jog respondentai tekstinę privatumo politikos išdėstymą laiko pertekliniu, nutolusiu nuo teikiamų paslaugų, sunkiai perprantamu, atgarsiu ir skatinančiu sutikti su nuostatais jų neskaičius. Privatumo politikos nuostatų perskaitymas respondentams nebuvo tolygus supratimui. Tokiu atveju, kai kurios organizacijos renkasi vizualinius sprendimus. Vartotojai yra labiau linkę susipažinti su privatumo politikos nuostatais, jei jie yra pateikti grafiškai, o ne tekstiniu būdu (Paspatis, Tsohou ir Kokolakis, 2018). Tokiu būdu vartotojams nereikia perskaityti visų privatumo politikos nuostatų, kurie būna labai ilgi, galintys sukelti vartotojų susierzinimą. Vizualiai pateiktos pagrindinės privatumo politikos nuostatos padeda greičiau suvokti, ar mobiliąją aplikaciją nepažeidžia suvokiamos rizikos vartotojų duomenų saugumu, ir padeda priimti sprendimą įsidiesti aplikaciją arba ieškoti pakaitalų (Zhao ir kt., 2016).

Atliktose empirinėse studijose dažnai nagrinėjamas privatumo politikos vizualizacijos modelis (angl. Privacy Policy Visualization Model – trump. PPVM), kuris padeda supaprastinti privatumo politikos nuostatų pateikimą, suteikia išsamumą ir padeda vartotojams priimti sprendimus (Ghazinour ir Albalawi, 2016). Grafinis privatumo politikos atvaizdavimas vartotojams suteikia pridėtinės vertės ir

edukuoja apie duomenų apsaugos naudas ir pasekmes (Jones ir kt., 2017). Wilkinson., Bahirat, Namara, Lyu, Alsubhi, Qiu, Wisniewski ir Knijnenburg (2020) pabrėžia, jog privatumo politikos nuostatų pateikimas vizualiai leidžia vartotojams iš karto pastebėti, kokie duomenys bus renkami, o tai teigiamai veikia vartotojų tolimesnį elgesį bei pasitikėjimą. Wilkinson ir kt., (2020) atliktame vartotojams priimtinių ir suprantamų mobiliųjų aplikacijų duomenų rinkimo informacijos pateikimo vizualiai empiriniame tyrime rezultatai parodė, kad grafiškai pateikiami privatumo politikos nuostatai bei renkami duomenys vartotojams padeda efektyviau apdoroti informaciją ir ją suprasti. Šiam teiginiui pritaria ir kiti tyrėjai, teigdami, kad pateikti trumpi privatumo politikos nuostatai taupo vartotojų laiką ir suteikia daugiau žinių apie privatumo praktiką (Meier, Schäwel ir Krämer, 2020). Be to, grafinis privatumo politikos nuostatų pateikimo formatas padeda atkreipti vartotojų dėmesį ir imtis veiksmų, leidžia pastebėti neįprastą aplikacijų elgesį su duomenimis, padeda užkirsti kelią pažeidimams, vartotojams leidžia sustiprinti tam tikros rūšies duomenų apsaugą, jei vartotojas jaučią poreikį tai padaryti (Wilkinson ir kt., 2020). Autoriai Jones ir kt. (2017) pažymi, kad vizualiniam privatumo politikos apipavidalinimui svarbu atsižvelgti į:

1. Pateiktų nuostatų skaidrumo aprašymą (Brandtzaeg, Pultier ir Moen, 2018)
2. Informacijos supaprastinimą tiek, kad vartotojai suprastų pateiktos informacijos vertę ir naudą. BDAR teigiama, kad organizacijoms privaloma mažinti pateiktų duomenų apsaugos nuostatų kiekį (Europos Parlamento ir Tarybos reglamentas), kuris vis dar vyrauja kai kuriose el. platformose ar mobiliosiose aplikacijose.
3. Nuostatų atvaizdavimo pritaikymą pagal aplikacijos kategoriją. Vartotojai tampa atribojami nuo perteklinės informacijos ir gauna tik tikslingai atrinktą informaciją;
4. Galimybę pasirinkti sutikimus. Gerinant vartotojų patirtį, vizualiai pateikta privatumo politika, atsižvelgiant į BDAR reikalavimus, turi leisti vartotojams ne tik galimybę atsisakyti arba priimti sutikimą, bet ir leidimą atsirinkti, ką norima patvirtinti (Ghazinour ir Albalawi, 2016; Jones ir kt., 2017).
5. Personalizaciją. Vartotojams sutikus su tam tikrais nuostatais, būtų aiškiai pranešama kokia informacija su kuo buvo pasidalinta, ir kaip bus apie tai pranešama (Wilkinson ir kt., 2020).

Kitų autorių tyrimuose personalizacija nebuvo reikšmingas veiksnys, jei prieš ketinant įsidiegti mobiliąsias aplikacijas. Pateikiama vizuali informacija, susijusi su aplikacijos saugumu, paveikia ketinimą rinktis saugesnes aplikacijas bei keičia vartotojų elgesį duomenų saugumo atžvilgiu (Chong ir kt., 2018).

Jones ir kt. (2017) empirinio tyrimo rezultatuose respondentai įvardijo šiuos vizualinius privatumo politikos aspektus, kurie paskatino tyrimo dalyvius labiau įsitraukti į susipažinimą su privatumo politikos teiginiais:

1. Lengvai suprantamos kategorijos ir paprastas išdėstymas;

2. Aiški ir įtraukianti privatumo politikos kalba;
3. Detalumas;
4. Raginimas veikti;
5. Bendras žaismingumas (spalvos, adaptyvus dizainas).

Be to, Jones ir kt. (2017) tyrimo respondentai teigė, jog toks privatumo politikos vizualinis pateikimas leido geriau suprasti įmonės duomenų apsaugos praktiką. Pagrindines privatumo politikos duomenų apsaugos praktikos gali būti suprantamos kaip: paaiškinimas, kaip ir kodėl renkama informacija, duomenų dalinimasis su trečiosiomis šalimis, suteikiama galimybė kontroliuoti renkama informaciją, vartotojų galimybė būti pamirštiesiems, prieiga prie anketos/duomenų valdymo bei redagavimo, suteikiama informacija, kiek laiko bus saugomi asmens duomenys, informacija apie duomenų apsaugą, informavimas apie privatumo politikos pokyčius, informacija, kaip ir kada duomenys bus sekami, papildomi nuostatai tam tikroms vartotojų grupėms (pvz.: vaikams, skirtingų privatumo politikos režimų gyventojams) ir kitos kategorijos, kurios neįeina į pagrindines (Wilson, Schaub, Dara, Liu, Cherivirala, Leon, Andersen, Zimmeck, Sathyendra, Russell, Norton, Hovy, Reidenberg ir Sadeh, 2016). Vartotojams adaptyvus ir priimtinas privatumo politikos informacijos pateikimas turėtų užtikrinti modalumą, vartotojų įgalintą kontrolę, personalizavimą, pasitikėjimą, maksimalų suprantamumą (Limba ir kt., 2020). Be to, pateikiami nuostatai turi būti susiję su teikiamomis paslaugomis (Jones ir kt., 2017).

Kitų autorių tyrimuose vaizdo įrašo formatu pateikti privatumo politikos nuostatai bei jų paaiškinimai, turėjo panašius rezultatus bei tikslus kaip ir grafinis pateikimas. Tyrime išvelgiama, kad vaizdo įrašo būdas padeda vartotojams sukurti pasitikėjimo organizacija išpūdį bei supaprastina teisine kalba pateikiamus tekstus (Wood, 2019). Tačiau šis privatumo politikos būdas moksliniuose tyrimuose buvo ne itin detalai analizuojamas lyginant su grafiniu vaizdavimu.

Taigi, privatumo politikos teiginiai turi atspindėti naujausio BDAR nuostatus. Vartotojams įprasta tekstiniu pavidalu išdėstoma privatumo politikos informacija ne visada įtraukia vartotojus ją perskaityti. Toks būdas nesukuria stimulo suprasti bei sužinoti duomenų tvarkymo ir panaudojimo principus. O tai yra ypač svarbu asmenims, kurie turi aukštą duomenų apsaugos suvokimą. Aiškumo ir supaprastinimo tikslui pasiekti, organizacijos eksperimentuoja su skirtingais privatumo politikos nuostatų pateikimo formatais. Tai gali būti dinamiškai, estetiškai ir grafiškai pateikta duomenų apsaugos informacija. Toks pateikimo būdas stiprina pasitikėjimą organizacijos veikla ar mobiliąja aplikacija. Be to, atsižvelgiant į vartotojo sąsają su mobiliąja aplikacija, svarbu atsižvelgti į aplikacijos kategoriją. Darbe nagrinėtos mokslinės literatūros išvados leido suprasti, kad skirtingos aplikacijų kategorijos skirtingai veikia vartotojų suvokiamas rizikas ir pasitikėjimą. Todėl kai kurios informacijos pateikimo savybės ar privatumo politikos pateikimo formatai, priklausomai nuo aplikacijos kategorijos, gali turėti didesnę reikšmę nei kiti. Šio darbo tyrimo analizei bus naudojamas skirtingas privatumo politikos

pateikimo formatas, tyrimo anketoms pritaikomas skirtingas privatumo politikos rizikos indeksas.

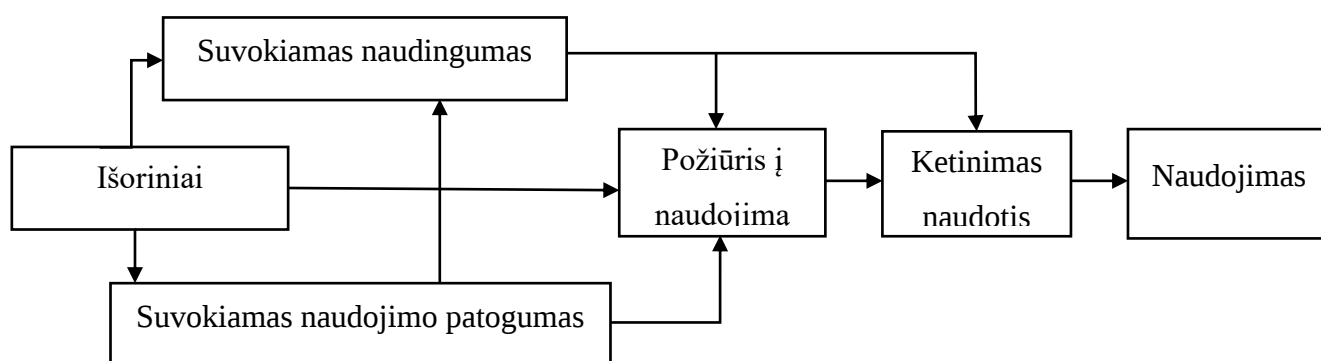
1. 5. Vartotojų ketinimą įsidiesti mobiliąsias aplikacijas aiškinantys modeliai

Įspėjimai apie duomenų rinkimą ir panaudojimą yra skirti paveikti vartotojų elgesį (Wilkinson ir kt., 2020). Aiškus privatumo politikos nuostatų išdėstymas ir susipažinimas su jomis padeda išvengti duomenų apsaugos pažeidimų. Įprastai, vartotojai nėra linkę jų perskaityti, tačiau tai gali priklausyti ir nuo vartotojų susirūpinimo jų duomenų saugumu lygmenis. Prieš priimant sprendimą įsidiesti aplikacijas, vartotojai turi tam tikrus išankstinius įsitikinimus ir motyvaciją. Susirūpinimas duomenų saugumu gali būti aukštas arba žemas, todėl svarbu suprasti, kokie veiksniai padeda sumažinti suvokiamą riziką duomenų saugumu. Aplikacijos, kuriose privatumo politikos įgyvendinimas yra žemas, gali būti pakeičiamomis konkurentų aplikacijomis. Remiantis mokslinė literatūros analize, asmens duomenų apsaugos užtikrinimas naudingas mobiliųjų aplikacijų kūrėjams, siekiant išsiskirti iš konkurentų, kurti vartotojų pasitikėjimą bei teikti kokybiškas paslaugas. Vartotojų požiūriu, tai duomenų apsaugos teisių užtikrinimas, suvokiamas saugumas internetinėje erdvėje bei vartotojų pasitenkinimo kėlimas.

Atlikus mokslinės literatūros analizę, pastebima, kad prieš ketinant įsidiesti mobiliąsias aplikacijas, vartotojai duomenų apsaugą sieja su: pasitikėjimu aplikacijos kūrėju bei jo reputacija, aplikacijos vertė pačiam vartotojui, informacijos kokybė ir aiškumu, galimybe valdyti asmens duomenis ir kitais veiksniais. Tačiau daugelyje atliktų tyrimų neanalizuojama, kaip šie veiksniai paveikia būsimo vartotojų apsisprendimą ir elgesį esant skirtingai aplikacijos kategorijai ir informacijos jautrumui. Daugelis autorių ketinimui įsidiesti aplikacijas veikiančius veiksniai ir vartotojų elgesį aiškina technologijų priėmimo modeliu (angl. TAM – Technology Acceptance Model).

1 paveikslas

TAM modelio struktūra



Šaltinis: sudaryta autorės pagal Cheng (2018); Kristadi ir Sucahyo (2016).

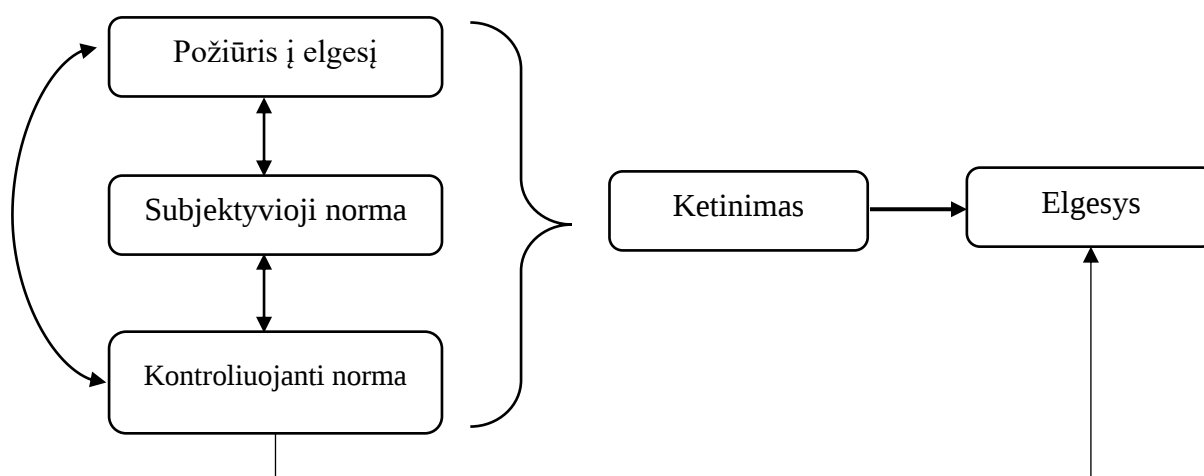
TAM modelis aiškina, jog ketinimą naudotis technologijomis veikia suvokiamas naudingumas

ir vartojimo patogumas (Davis, 1989). Remiantis Davis (1989), šie ketinimą naudotis technologijomis veikiantys veiksniai vartotojams sukuria teigiamos patirties suvokimą. Jei vartotojai dominančias mobiliąsias aplikacijas suvoks kaip komplikuojančias darbą ar ribojančias teigimą naudotimosi patirtį, vartotojų sąmonėje susidarys neigiamas požiūris į technologinį pranašumą, todėl bus nebesvarstoma naudotis jomis. Susidaręs teigiamas požiūris į aplikacijas veikia ketinimą jomis pasinaudoti, o tai lemia technologijų priėmimą.

Pasak Kim ir kt. (2014), tiriant ketinimą naudotis technologijomis vien tik TAM modelio nepakanka. Autoriai pabrėžia, kad TAM modelis negali apimti visų vartotojų elgesio veiksnių. Todėl tiriant ketinimą įsidiesti aplikacijas tyrimuose taip pat naudojama planuotos elgsenos teorija (angl. TPB – Theory of Planned Behaviour). TPB modelis ne tik padeda suvokti vartotojų elgesį, bet ir leidžia įvertinti pasitikėjimą (Giampietri, Verneau, Del Giudice, Carfora ir Finco, 2018).

2 paveikslas

Planuotos elgsenos teoriją aiškinantis modelis



Šaltinis: Ajzen (1991)

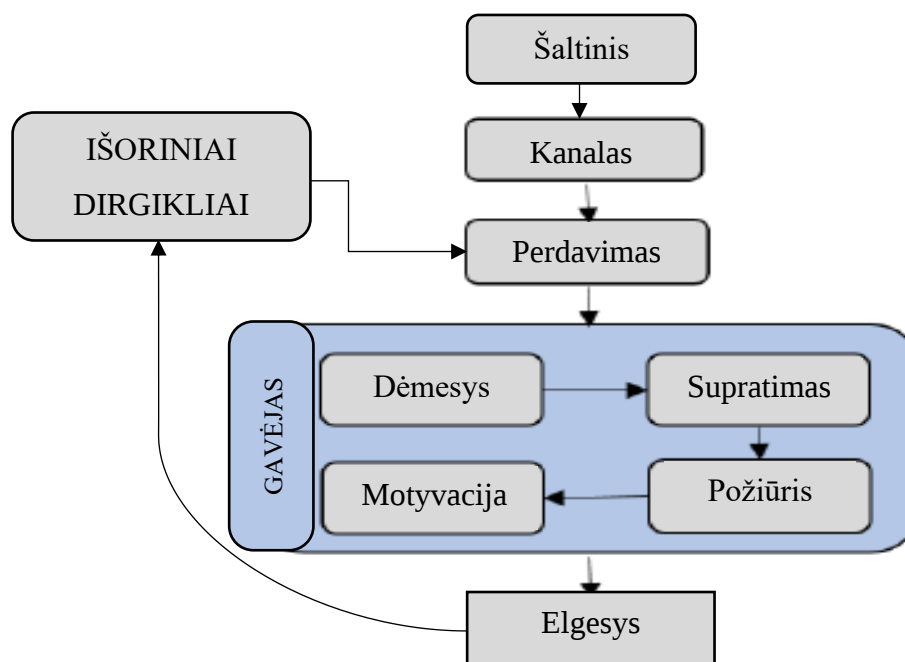
Remiantis planuotos elgsenos teorijos sudarytoju ir taikymo pradininku Ajzen (1991), pagrindiniu modelio konstruktu laikomas ketinimas, kurį galima prilyginti žmogaus motyvacijai. Pirmasis modelio konstruktas – požiūris. Jis gali būti suprantamas kaip tam tikras asmens palankumas arba nepalankumas tam tikram elgesiui (Ajzen, 1991). Subjektyvioji norma suprantama kaip subjektyvus asmens elgsenos situacijoje, atsižvelgiant į esamą požiūrį. Kontroliuojanti norma apibūdinama kaip suvokiamas sudėtingumas arba paprastumas prieš nusprendžiant kaip elgtis (Ajzen, 1991). TPB modeliu tyrimuose yra matuojamas kognityvinis asmenų elgsenos.

Kai kuriuose empiriniuose tyrimuose privatumo politikos informacijos adaptavimas ir įspėjimų pateikimas, siejamas su mobiliosiomis aplikacijomis, aiškinamas C-HIP arba žmogaus informacijos apdorojimo (angl. Communication-Human Information Processing) modeliu. Šis modelis taip pat matuoja vartotojų ketinimus bei elgesį priimant ir apdorojant pateikiamą įspėjančią informaciją. Modelis

yra pagrįstas grįžtamojo ryšio kilpos principu. Informacija keliauja nuo šaltinio ir pasireiškia tam tikru elgesiu bei elgesys taip pat veikia patį pirminį šaltinį (Chen, 2020; Wogalter, 2018).

3 paveikslas

C-HIP modelio struktūra



Šaltinis: sudaryta autorės pagal Wilkinson ir kt., (2020); Wogalter, Mayhorn, Black, Luna, Lund ir Walker (2017)

Pasak Chen (2020), C-HIP modeliu nėra aiškinamas tik informacijos perdavimo bei supratimo kelias, taip pat yra matuojami kognityviniai-afektyviniai bei socialiniai-kognityviniai komponentai. C-HIP modelis pradedamas aiškinti nuo šaltinio. Šaltinis gali būti suprantamas kaip bet koks subjektas, įspėjantis apie galimas rizikas (Wogalter, 2018). Įspėjanti informacija perduodama įvairiais kanalais, kuri pasiekia informacijos gavėją. Kad informacija būtų suprasta, ji turi patraukti vartotojų dėmesį. Šiame etape informacijos pateikimas yra ypač svarbus. Dėmesį pritraukiantis pateikimas padeda vartotojams atsiriboti nuo išorinių dirgiklių, susitelkiant ties susidomėjimu informacija (Wogalter, 2018). Esant pakankamai aiškiai išdėstytai informacijai, vartotojai susidaro tam tikrą požiūrį į informacijos svarbą, kas gali lemti ketinimą įsidiegti aplikacijas, supratęs ir priėmus galimas duomenų saugumo rizikas.

Felt ir kt. (2012) atliktame tyrime apie aplikacijos suteikiamų leidimų kaip naudingų saugumo rodiklių svarbą, užtikrinant perteikiamos informacijos skaidrumą bei tikslumą įsidiegiant aplikacijas, C-HIP modelis yra aiškinamas bei suskirstomas į šias kategorijas bei tikslus:

1. Vartotojų dėmesys: ar vartotojai atkreipia dėmesį leidimus prieš įsidiegiant aplikacijas? Autoriai Felt ir kt. (2012) šį modelio etapą aiškina kaip vartotojų gebėjimą bei poreikį atkreipti dėmesį į prašomus suteikti leidimus, atsiribojant nuo pagrindinio tikslo – aplikacijos įsidiegimo. Šiame etape vartotojai turi turėti pakankamai laiko perskaityti ir suprasti leidimų esmę.

2. Supratimas: šiame etape vartotojai turi suprasti leidimų bei aplikacijos tarpusavio ryšio rizikas. Vartotojams būtina suprasti leidimų apimtį ir pasekmes (Felt ir kt., 2012).

3. Požiūris ir įsitikinimai: šiame etape vartotojams būtina suprasti, ar leidimai perteikia tikrąsias rizikas.

4. Motyvacija: šiame modelio pritaikymo etape turima suprasti, ar vartotojams rūpi jų įrenginių saugumas, ar vartotojai yra motyvuoti apsvastyti leidimus (Felt ir kt., 2012).

5. Elgsena: paskutiniame etape svarbu įsitikinti, kokia įtaka leidimai turi apsisprendimui įsidiesti aplikacijas. Ar dėl perteklinių leidimų vartotojai atsisakytų ketinimo įsidiesti aplikacijas?

Analizuoti vartotojų ketinimus bei elgesį aiškinantys modeliai papildo vienas kitą skirtingais kintamaisiais. Technologijų priėmimo modelis matuoja suvokiamo naudingumo ir patogumo koreliaciją, veikiančią ketinimus bei elgesį. TAM modelį galima sieti su technologijų naudingumo požiūrio susidarymu, veikiančiu ketinimą. Planuotos elgsenos modelis aiškina elgesio, normų ir kontrolės tarpusavio ryšio poveikį ketinimams bei elgesiui. TPB modeliu yra matuojamas tikrasis vartotojų elgesys. C-HIP modeliu aiškinama informacijos perdavimo bei priėmimo eiga ir jos adaptavimas, norint komunikuoti apie galimas rizikas. Visi šie modeliai yra siejami su kognityviniu vartotoju elgesiu bei sprendimų priėmimu. Analizuoti modeliai leidžia suprasti veiksnius, veikiančius ketinimus, vartotojų požiūrį bei motyvaciją privatumo politikos bei renkamų duomenų informacijos pateikimo formatų atžvilgiu. Šiame skyriuje išnagrinėtais vartotojų ketinimą bei elgseną aiškinančiais modeliais, bus konstruojamas darbo tyrimo modelis bei kintamųjų sąveika.

2. KETINIMO ĮSIDIEGTI APLIKACIJAS TYRIMO METODIKA

2. 1. Empirinio tyrimo tikslas, uždaviniai, modelis ir hipotezės

Remiantis atlikta mokslinės literatūros analize, šiame skyriuje pateikiamas sudarytas tyrimo modelis bei iškeltos hipotezės, tyrimo tikslas, uždaviniai. Remiantis šiuo modeliu, bus siekiama atlikti tyrimą darbo tikslui pasiekti.

Tyrimo tikslas – nustatyti, kokie privatumo politikos informacijos pateikimo formatai labiausiai paveikia vartotojų apsisprendimą įsidiegti mobiliąsias aplikacijas, priklausomai nuo skirtingos aplikacijų kategorijos. Tyrimo tikslui pasiekti, teorinėje dalyje nagrinėjami panašios tematikos tyrimų rezultatai, naudoti kintamieji.

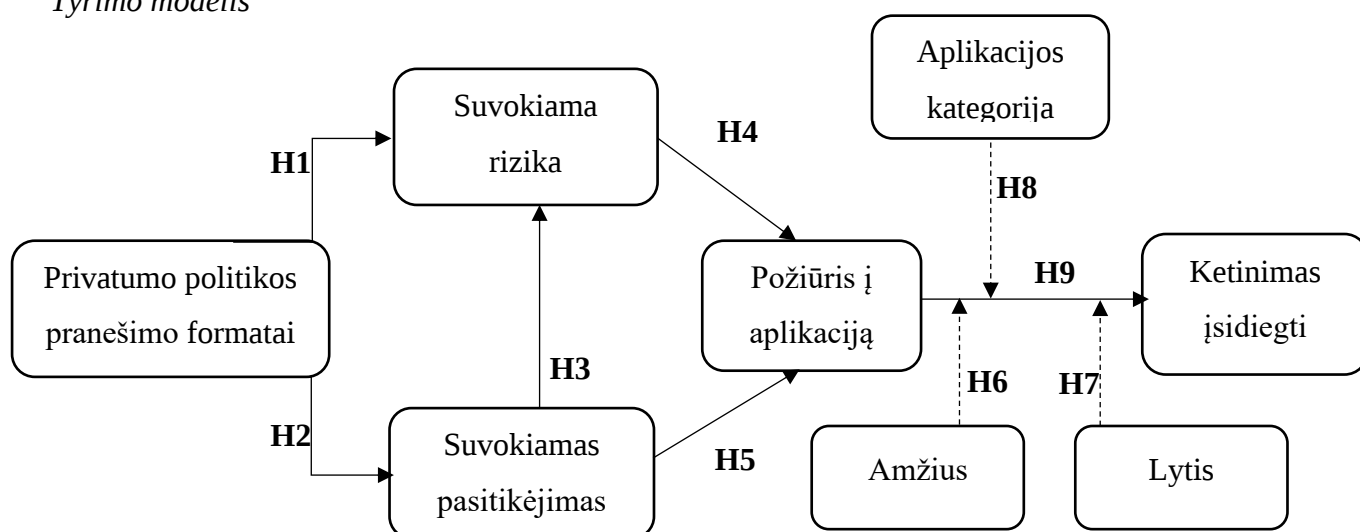
Tyrimo uždaviniai:

1. Išsiaiškinti vartotojų suvokiamos rizikos duomenų saugumu lygį;
2. Nustatyti vartotojų požiūrį į aplikacijas;
3. Išsiaiškinti vartotojų požiūrį į suvokiamas rizikas ir pasitikėjimą aplikacija;
4. Ištirti privatumo politikos informacijos pateikimo formatų poveikį, veikiantį ketinimą įsidiegti aplikacijas.

Iškelti uždaviniai bus įgyvendinami remiantis sudarytu tyrimo modeliu. Šį tyrimo modelį sudaro tokie nepriklausomi kintamieji kaip: privatumo politikos pateikimo formatai. Priklausomas kintamasis šiame modelyje – ketinimas įsidiegti aplikaciją. Nepriklausomas kintamasis – privatumo politikos pateikimo formatai. Medijuojančiais veiksniais išskirti: požiūris į aplikaciją, suvokiama rizika, suvokiamas pasitikėjimas. Moderuojantys veiksniai: aplikacijos kategorija, lytis, amžius.

4 paveikslas

Tyrimo modelis



Šaltinis: sudaryta autorės, remiantis atlikta mokslinės literatūros analize

Tyrimo hipotezės:

Tyrimuose teigiama, jog privatumo politikos pateikimo formatai bei informacijos pateikimo savybės leidžia geriau suprasti duomenų apsaugos praktikas (Jones ir kt., 2017). Vizuali pateiktis tampa įrankiu įvertinti galimas aplikacijos rizikas ir paveikti vartotojų elgesį (Wilkinson ir kt., 2020). Wilkinson ir kt. (2020) teigia, kad vartotojams svarbi tiek į duomenis, tiek į aplikaciją nukreipta informacija. Pasak tyrėjų, būsimiems vartotojams pateikiama su duomenų saugumu susijusi informacija padeda susidaryti bendrą rizikos suvokimą. Empiriniuose tyrimuose taip pat pabrėžiama, kad vartotojai labiau atkreipia dėmesį į pateikiamą vidutinį arba aukštą privatumo lygį (Tsai ir kt., 2011). Taip pat, suvokiamas privatumo politikos veiksmingumas yra neigiamai susijęs su mobiliųjų aplikacijų suvokiama privatumo rizika (Balapour ir kt., 2020). Išpėjimas apie galimas rizikas didina vartotojų susirūpinimą, tačiau nenaudojant riziką pabrėžiančio ženklavimo ar ikonų, vartotojai negalėtų iki galo suprasti aplikacijos rizikos ar ją neteisingai interpretuoti (Rajivan ir Camp, 2016). Remiantis tyrimų įžvalgomis, keliama prielaida, kad:

H1: Privatumo politikos pranešimo formatų pateikimas teigiamai sąlygoja suvokiamą riziką.

Vartotojai yra labiau linkę įsidiegti tas aplikacijas, kurios mobiliųjų aplikacijų parduotuvėse pateikiamos kaip patikimos (Harris ir kt., 2015b). Atsižvelgiant į keliamus reikalavimus privatumo politikos pateikimui, teisingai juos pateikus, vartotojai suvokia, jog jų duomenimis yra rūpinamasi, o tai sukelia vartotojų pasitikėjimą. Vyraujantis kuo didesnis suvokiamas saugumas platformomis didina vartotojų pasitikėjimą (Flavián ir Guinalíu, 2006). Mobiliųjų aplikacijų privatumo politikos veiksmingumas teigiamai veikia suvokiamą mobiliųjų programėlių saugumą (Balapour ir kt., 2020). Šiam teiginiui pritaria ir kiti autoriai. Tsai ir kt. (2011) empirinio tyrimo rezultatuose teigiama, kad turi būti atmetama galimybė, jog vartotojai priimtų sprendimus remdamiesi vien ikonų buvimu pateikiant privatumo politikos nuostatus nepaisant jų reikšmės. Remiantis atliktų tyrimų pagrindu, keliama hipotezė, jog:

H2: Privatumo politikos pranešimo formatų pateikimas teigiamai sąlygoja suvokiamą pasitikėjimą.

Balapour ir kt. (2020) tyrimo rezultatuose teigiama, kad vartotojams suvokiamas privatumo politikos supratimas mažina suvokiamą riziką bei veikia mobiliųjų aplikacijų saugumo supratimą. Liao, Liu ir Chen (2011) teigia, kad suvokiama rizika neigiamai koreliuoja su suvokiamu pasitikėjimu. Be to, tyrimuose pabrėžiama, kad suvokiama rizika bei suvokiamas pasitikėjimas dažnai veikia tarpusavyje (Liao, Liu ir Chen, 2011). Kiti autoriai taip pat pritaria šiam ryšiui, teigdami, kad suvokiamas pasitikėjimas sumažina rizikos suvokimą (Zimmer, Arsal, Al-Marzouq ir Grover, 2010). Remiantis atliktų tyrimų pagrindu, keliama hipotezė, jog:

H3: Suvokiamas pasitikėjimas turi neigiamą ryšį su suvokiama rizika.

Remiantis Balapour ir kt. (2020) atlikto tyrimo apie suvokiamą privatumo kaip saugumo

užtikrinimo veiksnį rezultatais, vartotojų suvokiama rizika neigiamai veikia suvokiamą mobiliųjų aplikacijų saugumą. Norint greičiau priimti sprendimą įsidiesti aplikaciją, vartotojams svarbu, kad informacija apie galimas rizikas būtų prieinama (Tay ir kt., 2021). Empiriniuose tyrimuose teigiama, kad suvokiama rizika duomenų apsauga neigiamai veikia požiūrį į aplikacijas (Lai ir kt., 2018). Todėl keliama prielaida, kad:

H4: Suvokiama rizika neigiamai sąlygoja požiūrį į aplikaciją.

Empiriniuose tyrimuose teigiama, kad daugelis vartotojų perskaito atsiliepimus apie aplikacijas bei peržiūri kitus aplikacijos kokybę bei saugumą indikuojančius parametrus (Harris ir kt., 2015a). Pasak Shin (2010), kuo labiau užtikrinamas vartotojų pasitikėjimas, tuo mažiau pastangų reikia internetinės svetainės ar aplikacijos vertinimui. Pasitikėjimas aplikacijų valdytoju teigiamai veikia ketinimą naudotis aplikacijomis (Namara ir Knijnenburg, 2021) bei pozityviai veikia bendrąjį požiūrį į aplikacijas (Setiawan ir Widanta, 2021). Taigi, prieš įsidiędiant aplikacijas, vartotojai turi susidare tam tikrą pasitikėjimo lygmenį. Suvokiamas pasitikėjimas padeda vartotojams suvokti, ko galima tikėtis iš aplikacijos saugumo atžvilgiu. Remiantis autorių įžvalgomis, keliama hipotezė, jog:

H5: Suvokiamas pasitikėjimas sąlygoja požiūrį į aplikaciją.

Daugelyje autorių tyrimų pabrėžiamas svarbus lyties vaidmuo, tačiau, teigiama, jog skirtingas vartotojų amžius taip pat veikia suvokiamą pasitikėjimą aplikacijos saugumu (Balapour ir kt., 2020) bei ketinimą įsidiesti aplikaciją (Hassandoust, Akhlaghpour ir Johnston, 2020). Bergström (2015) tyrimo rezultatuose teigiama, kad jaunesni žmonės šiek tiek labiau nei vyresni nerimauja dėl privatumo socialiniuose tinkluose, o naudojantis elektronine bankininkyste – atvirkščiai. Todėl keliama prielaida, kad:

H6: Amžius sąlygoja susidariusio požiūrio į aplikaciją įtaką ketinimui ją įsidiesti.

Pasak Chen, Yan, Fan ir Gordon (2015) tyrimo rezultatų, suvokiama rizika skiriasi priklausomai nuo lyties. Autorių rezultatuose taip pat minima, jog vyrai, turintys didesnę polinkį į pasitikėjimą, suvokia didesnę riziką nei moterys. Remiantis autorių įžvalgomis, sudarytas bendras rizikos ir pasitikėjimo požiūris į aplikaciją turėtų skirtis nuo lyties svarstant ketinimą įsidiesti. Nagrinėtuose šaltiniuose lytis įvardijama kaip vienas iš svarbesnių moderuojančių ryšių kintamųjų. Dėl šių priežasčių keliama hipotezė, jog:

H7: Lysis sąlygoja susidariusio požiūrio į aplikaciją įtaką ketinimui ją įsidiesti.

Kai kuriuose tyrimuose teigiama, kad skirtinga aplikacijos kategorija (utilitarinė ar hedoninė) nevienodai veikia vartotojų pasitikėjimą pateikiant jautrius duomenis (Jones ir kt., 2017). Hong ir Thong (2013) tyrimo rezultatų išvadose taip pat pabrėžiamas nevienodas vartotojų suvokimas bei susirūpinimas renkama duomenimis esant skirtingoms interneto platformoms. Atliktuose panašiuose tyrimuose buvo daroma prielaida, kad suvokiamą riziką duomenų saugumu veikia skirtinga mobiliųjų aplikacijų kategorija (Chang ir kt., 2018; Malik ir kt., 2017). Susirūpinimas privatumu skaitmeninėje erdvėje yra

susijęs su asmeniškėmis programomis, tokiomis kaip socialiniai tinklai ir internetinė bankininkystė, o bendro pobūdžio aplikacijos sukelia mažiau nerimo (Bergström, 2015). Remiantis atliktų tyrimų pagrindu, keliama hipotezė, jog:

H8: Aplikacijos kategorija sąlygoja susidariusio požiūrio į aplikaciją įtaką ketinimui ją įsidiesti.

Sudarytas požiūris ir žinojimas apie aplikacijos funkcionalumus bei rizikas turi įtakos ketinimui įsidiesti aplikaciją (Hammouri ir kt., 2020). Be to, atliktuose tyrimuose teigiama, kad suvokiamas teigiamas aplikacijos naudingumas veikia ketinimą įsidiesti aplikacijas (Lai ir kt. 2018; Hassandoust ir kt., 2020; Hur ir kt., 2017). Suvokiama utilitarinė ar socialinė nauda skatina įsidiesti aplikacijas. Zhang ir kt. (2018) atliktame empiriniame tyrime teigiama, kad požiūris ir ketinimas įsidiesti mobiliąsias aplikacijas tarpusavyje koreliuoja. Taip pat tyrimuose teigiama, jog bendras požiūris į aplikaciją teigiamai veikia vartotojų ketinimus (Sreejesh ir kt., 2016). Kiti autoriai taip pat pritaria, jog bendrąją prasme informacija apie privatumą veikia vartotojų sprendimų priėmimą (Tsai ir kt., 2011). Todėl keliama prielaida, kad:

H9: Požiūris į aplikaciją teigiamai sąlygoja ketinimą ją įsidiesti.

Kitame skyriuje pateikiamas tyrimo metodas, instrumentai, imtis bei tyrimo rezultatų patikimumas.

2. 2. Tyrimo metodai, instrumentai ir eiga

Tyrimui pasirinktas kiekybinis tyrimo metodas, 2x2x2 (du privatumo politikos pranešimo pateikimo tipai; utilitarinė ir hedoninė aplikacija; rizikinga ir nerizikinga aplikacija) faktorinė analizė. Panašiuose nagrinėtuose tyrimuose (Choi ir Land, 2016; Keith, Babb, Furner, Abdullat ir Lowry, 2016; Kitkowska, Warner, Shulman, Wästlund ir Martucci, 2020; Meier ir kt., 2020; Tay ir kt., 2021) taip pat buvo naudojamas faktorinis tyrimo dizainas, todėl galima teigti, kad toks metodas tikslui pasiekti yra priimtinas. Kiekybinis tyrimo metodas leidžia apklausti didesnę respondentų grupę bei pritaikyti rezultatus platesnei populiacijai. Taip pat teorinėje dalyje analizuojamuose tyrimuose daugelis mokslininkų naudojo kiekybinį tyrimo modelį.

Tyrimo instrumentas – internetinė anketinė apklausa. Tyrimo apklausos anketa buvo sukurta naudojantis “QuestionPro“ internetine anketų kūrimo svetaine (žr. 22 priedą). Apklausoje pateikiami uždari anketos klausimai. Į atvirus anketos klausimus respondentai nėra linkę atsakinėti, tai sukelia nepatogumą pildant anketinę apklausą, todėl uždari klausimai padeda surinkti daugiau duomenų. Taip pat uždaro tipo klausimus lengviau apdoroti statistinės analizės įrankiais, juos tampa lengviau palyginti (Gaižauskaitė ir Mikėnė, 2014, p. 166). Tokio tipo klausimai padeda išvengti tyrėjo bei respondentų interpretacijų į klausimus ir jų atsakymus. Vienintelis atviras klausimas buvo naudojamas surinkti demografinius respondentų duomenis, t.y. amžių. Šiame tyrime tiriamas informacijos pateikimo

poveikis ketinimui įsidięti mobiliąsias aplikacijas, todėl atliekant tyrimą nebuvo apsiribojama ties konkrečia amžiaus grupe, nes tyrimo problema yra taikoma plačiai populiacijos daliai. Klausimų konstruktais išmatuoti, pasitelkiamos 7 balų Likerto skalės, kai 1 – visiškai nesutinku, 2 – nesutinku, 3 – daugiau nesutinku, nei sutinku, 4 – nei nesutinku, nei sutinku, 5 – daugiau sutinku, nei nesutinku, 6 – sutinku, 7 – visiškai sutinku. Atlikus mokslinės literatūros analizę, keletas mokslininkų tolimesnei ketinimui įsidięti mobiliąsias aplikacija turintiems veiksniams tirti, siūlo pasitelkti 7 balų Likerto skales. Taip pat Likerto skalės padeda įvertinti nuostatas bei įsitikinimus (Bilevičienė ir Jonušauskas, 2011, p.22), kurie yra aktualūs šio darbo tikslui pasiekti.

Prieš pateikiant anketinės apklausos klausimus, buvo trumpai pristatomas tyrėjas bei tyrimo tikslas, mokymosi įstaiga, kurioje atliekamas tyrimas. Buvo minima, jog respondentų anonimiškumas yra užtikrinamas, o duomenys naudojami tik prieš tai įvardinto tyrimo tikslui pasiekti. Taip pat nurodomas preliminarus anketos užpildymo laikas – apie 10 minučių.

Pirmoje anketinės apklausos dalyje siekiama išsiaiškinti respondentų susirūpinimo savo privatumu lygį remiantis Westin indeksu. Antroje dalyje siekiama išsiaiškinti, kaip pateikti privatumo politikos pateikimo formatai yra geriau suprantami respondentams, priklausomai nuo skirtingos aplikacijų kategorijos. Trečioje anketos dalyje pateikiami klausimai demografiniams duomenims surinkti (lytis, amžius). Iš viso anketą sudarė 11 konstrukto ir 4 atskirtos anketos, sudarytos iš teorinėje dalyje nagrinėtų autorių tyrimų konstrukto teiginių. Anketoje respondentų buvo prašoma įvertinti suvokiamos rizikos, pasitikėjimo, vizualinio naudingumo teiginius, požiūrį į aplikaciją bei patį ketinimą įsidięti aplikacijas (žr. 1 lentelę). Anketose buvo pateikiamos situacijos A ir B. Kiekvienos anketos situacija apima skirtingą privatumo politikos informacijos pateikimo tipą, utilitarinę ir hedoninę aplikacijos kategoriją, privatumo pranešimo rizikingumo indeksą, kuriuo remiantis, vartotojams bus sudaromas rizikingos ir nerizikingos aplikacijos vaizdinys. Sudarant situacijas, stengiasi sukurti realų Android aplikacijų vaizdinį. Remiantis statistiniais duomenimis (Statista, 2021), lyginant populiariausias pasaulyje išmaniųjų įrenginių operacines sistemas yra pastebima, kad Android operacinė sistema yra ženkliai lyderiaujanti rinkoje lyginat su kitomis operacinėmis sistemomis. Dėl šios priežasties pasirinkta atvaizduoti Android operacinės sistemos aplikacijų vizualiką. Situacijose pateikiamas aplikacijų pavadinimas, nurodoma kategorija, PEGI (amžiaus tinkamumo) indeksas. Kiekvienai situacijai pateikiamas bazinius ES reikalavimus atitinkantis privatumo politikos pateikimo formatas, vizualus aplikacijos rizikingumo lygio atvaizdavimas. Pateikiami privatumo politikos nuostatai šiam tyrimui pritaikyti remiantis Kitkowska ir kt. (2020) bei Betzing ir kt. (2019) tyrimu, aplikacijos rizikingumo pateikimas pritaikytas remiantis Tay ir kt. (2021). Abiejų aplikacijų (utilitarinės ir hedoninės) pavadinimai buvo sugalvoti darbo autorės, nereferuojant į egzistuojančias aplikacijas ar jų pavadinimus.

Tyrimui pasirinkta tirti 2 skirtingo pobūdžio mobiliųjų aplikacijų kategorijas: kasdieninių

finansų bei socialinių tinklų. Šios skirtingos aplikacijų kategorijos pasirinktos dėl galimo skirtingo rizikų suvokimo, vartojimo tikslo bei skirtingo naudos suvokimo. Pasirinktos skirtingos mobiliųjų aplikacijų kategorijos padės suprasti hedoninius bei utilitarinius vartotojų rizikos suvokimus, susijusius su duomenų apsaugos rizika. Socialinių tinklų asmens duomenų saugumo klausimas yra ypač aktualus. Socialiniuose tinkluose ne tik pateikiama asmeninė informacija, tačiau tai ir tam tikra reklamos sklaidos platforma. Socialinių tinklų aplikacija atitinka hedoninę kategoriją. Kasdieninių finansų aplikacijos atitinka utilitarinius vartotojų poreikius. Tokio pobūdžio aplikacijos dažniausiai apima jautrių asmens duomenų rinkimą bei apdorojimą. Be to, remiantis teorinėje dalyje nagrinėtais moksliniais šaltiniais, tyrimuose mobiliosios bankininkystės aplikacijos buvo įvardijamos kaip stipriausią susirūpinimą duomenų saugumu turinčios aplikacijos.

Atsižvelgiant į teorinėje dalyje nagrinėtus mokslininkų empirinius tyrimus, daugelyje iš jų informacijos pateikimo pavyzdžiams pateikti naudojamos neegzistuojančios mobiliosios aplikacijos ar sukurtos išgalvotos aplikacijų „DEMO“ versijos. Todėl šiame tyrime atsisakyta pasirinkti konkrečias aplikacijas, kurios atitiktų pasirinktas tyrimo kategorijas dėl to, jog būsimi respondentai gali nesinaudoti konkrečiomis aplikacijomis arba apie jas būti susiformavę išankstinę nuomonę duomenų saugumo klausimais. Toks faktas galėtų iškreipti būsimų duomenų patikimumą. Šis sprendimas taip pat buvo priimtas atsižvelgiant į Kelley ir kt. (2013) atlikto tyrimo rezultatus, kai vartotojai rinkosi plačiai pasaulyje žinomą prekės ženklą – aplikaciją net ir esant vartotojams suvokiamam pertekliniam leidimui kiekviui. Tuo pačiu pagrindu, jog žinomos ir populiarios mobiliosios aplikacijos gali iškreipti duomenis, Tay ir kt. (2021) tyrime taip pat atsisakyta naudoti žinomus aplikacijų vardus.

1 lentelė

Anketoje naudoti konstruktai ir klausimai

Konstruktai	Klausimai	Šaltinis
Suvokiama rizika	1. Manau, kad ši aplikacija gali pakenkti mano privatumui 2. Manau, kad asmeninės informacijos pateikimas šiai aplikacijai galėtų sukelti daug neaiškumų 3. Manau, kad susidurčiau su daugeliu problemų, pateikęs (-usi) savo asmeninę informaciją šiai aplikacijai 4. Manau, kad asmeninės informacijos pateikimas šiai aplikacijai sukeltų daug galimų nuostolių 5. Pateikti asmeninę informaciją šiai programai būtų rizikinga 6. Manau, kad ši aplikacija perduos asmeninę informaciją be mano leidimo	Lai ir kt. (2018)
Požiūris į	1. Mano požiūris į šią aplikaciją yra teigiamas	Lai ir kt.

aplikaciją	1 lentelės tęsinys 2. Manau, kad ši aplikacija patenkins mano lūkesčius	(2018)
	3. Mano požiūris į šią aplikaciją yra priimtinas 4. Mano požiūris į šią aplikaciją yra malonus	
Suvokiamas pasitikėjimas	1. Šios aplikacijos kūrėjai būtų patikimi tvarkydami mano informaciją; 2. Šios aplikacijos kūrėjai pasakytų tiesą ir vykdytų pažadus susijusius su mano pateikta informacija; 3. Tikiu, kad šios aplikacijos kūrėjai tvarkydami informaciją, nepamirštų mano interesų; 4. Šios aplikacijos kūrėjai yra nuspėjami ir nuoseklūs informacijos naudojimo atžvilgiu; 5. Šios aplikacijos kūrėjai visada sąžiningai elgtųsi su klientais, kai reiktų naudoti mano pateiktą informaciją.	Kitkowska ir kt. (2020)
Ketinimas įsidiegti	1. Jei turėsiu galimybę, naudosisiu ši aplikacija 2. Tikėtina, kad naudočiau šią aplikaciją, kai ji man bus reikalinga 3. Manau, kad svarstyčiau įsidiegti šią aplikaciją 4. Aš ketinčiau įsidiegti šią aplikaciją 5. Tikriausiai rekomenduočiau šią aplikaciją savo draugams.	Lai ir kt. (2018) Kerviler ir kt. (2016) Kim, Ferrin ir Rao (2008)
Privatumo politikos pranešimų formato vertinimas	1. Manau, kad vizualizuotas aplikacijos privatumo pranešimas padėjo man rasti galimas grėsmes, su kuriomis galiu susidurti (vizualizuotiems pranešimams); Manau, kad pateiktas privatumo pranešimas padėjo man suprasti galimas grėsmes, su kuriomis galiu susidurti (nevizualizuotiems pranešimams); 2. Manau, kad vizualizuota aplikacijos ataskaita buvo lengvai skaitoma 3. Manau, kad aplikacijos vizualizuota ataskaita buvo lengvai suprantama	Paspatis ir kt. (2018)
Westin privatumo indeksas	1. Vartotojai prarado bet kokią kontrolę dėl įmonės renkamų duomenų ir asmeninės informacijos naudojimo 2. Daugelis įmonių tinkamai ir konfidencialiai tvarko asmeninę informaciją, kurią renka apie vartotojus.	Kumaraguru ir Cranor (2005)

	1 lentelės tęsinys	
	3. Galiojantys įstatymai ir organizacinė praktika užtikrina pagrįstą vartotojų privatumo apsaugos lygį šiandien.	

Šaltinis: sudaryta autorės, remiantis teorinėje dalyje nagrinėtais tyrimais

Tiriamųjų imtis: tiriamųjų imčiai nustatyti, naudojama neatsitiktinė patogioji atranka. Todėl tiriamųjų imtis buvo nustatyta pagal anksčiau atliktus panašaus pobūdžio tyrimus (žr. 2 lentelę).

2 lentelė

Ankstesnių tyrimų imties dydžio palyginimas

Tyrimo autorius	Imties dydis
Tam, Santos ir Oliveira (2018)	304
Harris ir kt. (2015a)	155
Chen ir kt. (2015)	295
Harris ir kt. (2015b)	286
Chin ir kt. (2018)	214
Harris ir kt. (2016)	128
Chang ir kt. (2018)	363
Shklovski ir kt. (2014)	187
Hammouri ir kt. (2020)	270

Šaltinis: sudaryta autorės, remiantis ankstesniais tyrimais

Anksčiau atliktų tyrimų imties vidurkis svyruoja apie 245 respondentus. Todėl šiame tyrime pasirinkta tirti 250 respondentų, įskaitant galimas paklaidas dėl neteisingai ar netinkamai užpildytų anketų.

Tyrimo laikotarpis: 2021 m. gegužės - spalio mėnesiai.

Tyrimo patikimumas: anketoje pateiktų konstrukto patikimumui ir vidiniam suderinamumui patikrinti buvo naudojamas Kronbacho alfa (angl. *Cronbach alfa*) koeficientas. Šis koeficientas taip pat buvo naudojamas ankstesniuose tyrimuose, nagrinėtuose teorinėje dalyje. Minimaliu priimtiniu *Cronbach alfa* koeficientu laikomi režiai nuo 0,7 iki 0,8 (Gaižauskaitė ir Mikėnė, 2014, p. 146). Esant per aukštam konstrukto teiginių suderinamumui, galima išmesti vieną teiginį iš konstrukto taip gaunant patikimesnius duomenis. Tyrimui pasirinkta patogioji atranka neleidžia duomenų pritaikyti visai populiacijai.

Tyrimo duomenų apdorojimas: gauti tyrimo duomenys apdoroti Excel ir IBM SSPS Statistics 26

statistinės analizės programa. Papildomai įdiegtas Process v4.0 by Andrew F. Hayes programos papildinys moderacijai/mediacijai apskaičiuoti. Duomenims analizuoti naudojama koreliacija, tiesinė regresija, moderacija, faktorinė ANOVA.

Anketų patikimumas:

3 lentelė

Konstrukto patikimumo bei suderinamumo patikrinimas remiantis Cronbach alfa koeficientu

Konstruktas	Konstrukto sudarančių klausimų skaičius	Cronbach alfa α
Suvokiama rizika	6	0,943
Požiūris į aplikaciją	4	0,934
Suvokiamas pasitikėjimas	5	0,922
Ketinimas įsidiesti	5	0,943
Privatumo politikos pranešimo formatai	3	0,878
Westin indeksas	2	0,787

Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Atlikus Cronbach alfa (α) koeficiento skaičiavimus, Westin indekso Cronbach alfa (α) koeficientas buvo žemesnis nei 0,7, neigiamas Cronbach alfa (α) koeficientas buvo gautas net ir atlikus Reverse (R) metodą vienam iš konstrukto klausimų. Skaičiuojant galutinį Westin indekso Cronbach alfa (α), buvo pašalintas vienas iš teiginių. Tolimesniuose skaičiavimuose naudojami visi 3 konstrukto klausimai tik respondentų pasiskirstymui apskaičiuoti (priklausymas fundamentalistų, pragmatistų ir nesusirūpinusių privatumu kategorijoms). Westin indeksas kitiems skaičiavimams nebuvo naudotas dėl paties konstrukto netinkamumo. Likusių konstrukto patikimumas yra aukštas, tačiau juos galime laikyti tinkamais.

Prieš atliekant hipotezių tikrinimą ir tolimesnę duomenų analizę, buvo atlikta Varimax pasuktos matricos faktorinė analizė (žr. 4 priedą). Pagal atliktus skaičiavimus, KMO=0.956, Bartlett's $p<0.001$ (žr. 4 priedą). Pagal gautus rezultatus, tolimesniems tyrimo skaičiavimams faktorinė analizė yra tinkama, multikolinerumo problemos nėra.

Kitame skyriuje atliekama tyrimo rezultatų analizė ir aptarimas.

3. TYRIMO REZULTATŲ ANALIZĖ IR APTARIMAS

3. 1. Tyrimo rezultatų analizė

Demografinė respondentų statistika: viso internetinėje apklausoje dalyvavo 324 respondentai. Prieš pradedant analizuoti surinktus duomenis, buvo pastebėti respondentų nurodyti amžiaus ekstremumai, atmestos ne iki galo užpildytos anketos. Dėl šių priežasčių į tyrimo rezultatų analizę neįtraukti 79 respondentų atsakymai, todėl toliau tyrime analizuojamos 245 respondentų anketos. Prieš atliekant tolimesnę analizę, visų anketų respondentų duomenys buvo apjungti į vieną. Siekiant įvertinti, ar nebuvo reikšmingų skirtumų tarp amžiaus ir lyties pasiskirstymo, buvo atliekamas šių kintamųjų skirtingose anketose įvertinamas (žr. 4 lentelę).

4 lentelė

Respondentų amžiaus ir lyties pasiskirstymas procentais skirtingose anketose, N=245

		Anketos			
		A	B	C	D
Amžius	Iki 29	87	66,7	70,4	73,8
	30-50	13	29,8	27,8	23,1
	51-98	-	3,5	1,9	3,1
Lytis	Moteris	58	47,4	50	46,2
	Vyras	42	52,6	50	53,8

Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Viso apklausoje dalyvavo 50,6% moterų bei 49,4% vyrų (žr. 1 priedą). Respondentų amžius, apimant visas anketas, pasiskirstė nuo 18 iki 59, amžiaus vidurkis 27 (26,91). Analizuojant duomenis, respondentai buvo suskirstyti į tris amžiaus kategorijas: nuo 18 iki 29 – I kategorija, nuo 30 iki 50 – II kategorija, nuo 51 iki 98 – III kategorija. Didžiausią respondentų procentinę (75,2%) dalį sudarė I-ai kategorijai priskirti respondentai. Skaičiavimai rodo, jog respondentų amžiaus bei lyties pasiskirstymas skirtingose anketose yra statistiškai reikšmingas ir tinkamas, todėl duomenis galima lyginti tarpusavyje.

Atliekant apklausas, buvo vertinamas A. Westin indeksas. Pirmasis teiginys „Vartotojai prarado bet kokią kontrolę dėl įmonės renkamų duomenų ir asmeninės informacijos naudojimo“ vertina, ar vartotojai yra fundamentalistai, turintys aukštą susirūpinimo duomenų apsaugos lygiu. Antrasis teiginys „Daugelis įmonių tinkamai ir konfidencialiai tvarko asmeninę informaciją, kurią renka apie vartotojus“ vertina, ar vartotojai yra pragmatistai, kuriems yra svarbi galimybė nuspręsti, ar jie nori atskleisti savo asmeninius duomenis. Trečiasis teiginys „Galiojantys įstatymai ir organizacinė praktika užtikrina pagrįstą vartotojų privatumo apsaugos lygį šiandien“ vertina nesusirūpinusius privatumu

vartotojus, kurie pasitiki įmonėmis, per daug neanalizuodami situacijos pateikia savo duomenis.

Atlikus T-testą, siekiant išsiaiškinti, ar vyrų ir moterų tarpe yra vidurkių skirtumas tarp respondentų, kurie priskiriami fundamentalistams, lyties atžvilgiu vidurkių skirtumo nebuvo (žr. 5 lentelę).

5 lentelė

Vyrų ir moterų pasiskirstymas priskiriamai fundamentalistų kategorijai

Westin indekso klausimas	Lytis	Imtis	Vidurkis	Standartinis nuokrypis	Stand. klaidos reikšmė	df	T-testo p
Westin 1 (R)	Moteris	248	4,15	1,658	0,105	488	0,122
	Vyras	242	3,92	1,591	0,102		

Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Taip pat papildomai buvo atliktas T-testas I-ajai ir II-ajai amžiaus kategorijoms. Šios kategorijos pasirinktos dėl didesnio respondentų skaičiaus šiose kategorijose lyginant su III-ąja kategorija. Be to, III-iosios amžiaus kategorijos respondentų skaičius lyginant su visa imtimi yra mažiausias. Taip pat nustatyta, jog amžiaus atžvilgiu nėra vidurkių skirtumo tarp respondentų, kurie priskiriami fundamentalistams (žr. 16 priedą).

Pakartojus T-testo skaičiavimus su antruoju Westin indekso teiginiu, nustatyta, kad amžiaus atžvilgiu nėra vidurkių skirtumo tarp respondentų, kurie priskiriami pragmatistų kategorijai (žr. 17 priedą). Tačiau vyrų ir moterų tarpe yra vidurkių skirtumas tarp respondentų (žr. 6 lentelę).

6 lentelė

Vyrų ir moterų pasiskirstymas priskiriamai pragmatistų kategorijai

Westin indekso klausimas	Lytis	Imtis	Vidurkis	Standartinis nuokrypis	Stand. klaidos reikšmė	df	T-testo p
Westin 2	Moteris	248	4,10	1,427	0,091	488	0,044
	Vyras	242	4,36	1,405	0,090		

Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Atlikus T-testo skaičiavimus su trečiuoju Westin indekso teiginiu, nustatyta, kad amžiaus atžvilgiu nėra vidurkių skirtumo tarp respondentų, kurie yra nesusirūpinę privatumu (žr. 18 priedą). Taip pat vyrų ir moterų tarpe vidurkių skirtumo tarp respondentų nebuvo (žr. 7 lentelę).

7 lentelė

Vyrų ir moterų pasiskirstymas nesusirūpinusių privatumu kategorijai

Westin indekso klausimas	Lytis	Imtis	Vidurkis	Standartinis nuokrypis	Stand. klaidos reikšmė	<i>df</i>	T-testo <i>p</i>
Westin 3	Moteris	248	4,38	1,504	0,095	483,025	0,740
	Vyras	242	4,42	1,325	0,085		

Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Taigi, statistiškai reikšmingų vidurkių skirtumų tarp respondentų, turinčių aukštą susirūpinimo duomenų apsaugos lygį nėra nei lyties, nei amžiaus atžvilgiu. Vertinant pragmatistų kategoriją, buvo nustatytas skirtumas tarp vidurkių lyties atžvilgiu. Vyrams labiau nei moterims apsisprendimo galimybė prieš norit atskleisti savo asmeninius duomenis yra svarbesnė. Kaip ir aukštą susirūpinimo duomenų apsaugos lygį turinčių respondentų taip ir nesusirūpinusių privatumu vartotojų vidurkiai amžiaus ir lyties atžvilgiu nesiskyrė. Galima teigti, kad respondentų požiūrio pasiskirstymas yra tolygus. Nėra išsiskiriančios kategorijos, kuriai priklausytų didžioji dalis respondentų. Todėl atsakant į tolimesnius anketos klausimus apie suvokiamą riziką bei pasitikėjimą, požiūrį į aplikacijas, nebuvo reikšmingų respondentų požiūrių prieštaraivimų.

3. 2. Tyrimo hipotezių tikrinimas

Šiame skyriuje buvo tikrinamos tyrimo hipotezės, siekiant nustatyti, kokie privatumo politikos pranešimo pateikimo formatai labiausiai paveikia vartotojų apsisprendimą įsidiegti mobiliąsias aplikacijas, priklausomai nuo skirtingos aplikacijų kategorijos ir aplikacijos rizikingumo.

Pirmąją hipoteze siekiama išsiaiškinti, kaip yra veikiama vartotojų suvokiama rizika, pateikiant skirtingą privatumo politikos pranešimo formatą (vizualų ir nevizualų). Atlikus tiesinę regresiją, **H1 yra priimta**, pateikiamas skirtingas privatumo politikos pranešimas turi įtakos vartotojų suvokiamai rizikai $R^2=0.040$, $F(1)=20.247$, $p<0.001$ (žr. 5 priedą).

Remiantis Stjudento T-testo rezultatais, siekiant išsiaiškinti, kaip vizualus ir nevizualus privatumo politikos pranešimo pateikimo formatas veikia suvokiamą vartotojų riziką, nustatyta, kad suvokiama rizika yra didesnė, kai yra pateikiamas nevizualus ($M=4.0068$) privatumo politikos pranešimo formatas lyginant su vizualiu ($M=3.3973$). Stjudento T-testo $t(488)=-4.500$, $p<0.001$ (žr. 8 lentelę). Su išvadomis sutinka Tsai ir kt. (2011), teigdami, kad tinkamai pateikta privatumo informacija padeda atkreipti vartotojų dėmesį, saugumo ar privatumo pranešimų ikonos padeda priimti sprendimą. Be to, pastarieji autoriai pabrėžia, kad vartotojai yra labiau linkę atlikti konversijas, kai privatumo

pranešimas yra pateiktas nei jo visiškai nėra. Kitų autorių tyrimų rezultatuose taip pat pritariama su hipotezės išvadomis, jog vizualus privatumo pranešimo pateikimas veikia vartotojų elgesį bei padeda suprasti rizikas (Wilkinson ir kt., 2020).

8 lentelė

Stjudento T-testo rezultatai lyginant vizualų ir nevizualų privatumo politikos pranešimų formatų įtaką suvokiamai vartotojų rizikai

Privatumo politikos pateikimo formatas	Imtis	Vidurkis	Standartinis nuokrypis	df	p	t
Vizualus formatas	245	3,3973	1,52983	488	0,000	-4,500
Nevizualus formatas	245	4,0068	1,46807			

Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Antrąją hipotezę siekiama išsiaiškinti, kaip yra veikiamas vartotojų suvokiamas pasitikėjimas, pateikiant skirtingą privatumo politikos pranešimo pateikimą (vizualų ir nevizualų). Atlikus tiesinę regresiją, **H2 yra priimta**, pateikiamas skirtingas privatumo politikos pranešimas turi įtakos vartotojų suvokiamam pasitikėjimui $R^2=0.053$, $F(1)=27.041$, $p<0.001$ (žr. 6 priedą).

Remiantis Stjudento T-testo rezultatais, siekiant išsiaiškinti, kaip vizualus ir nevizualus privatumo politikos pranešimo pateikimo formatas veikia suvokiamą vartotojų pasitikėjimą, nustatyta, kad suvokiamas pasitikėjimas yra aukštesnis, kai yra pateikiamas vizualus ($M=4,5265$) privatumo politikos pranešimo formatas lyginant su nevizualiu ($M=3,9086$). Stjudento T-testo $t(488)=5,200$, $p<0.001$ (žr. 9 lentelę). Jones ir kt. (2017) sutinka su išvada, kad privatumo politikos dizainas ženkliai didina vartotojų pasitikėjimą, vartotojai tampa labiau supažindinti su taikomomis privatumo praktikomis. Taip pat teigiama, kad orientuotas į vartotoją privatumo pranešimas sumažina privatumo praktikų interpretavimą, kas padeda sustiprinti pasitikėjimą. Todėl pasitelkiant vizualizacijas pateikiant privatumo pranešimus, didinamas suvokiamas saugumas ir vartotojų pasitikėjimas aplikacijomis (Flavián ir Guinalíu, 2006).

9 lentelė

Stjudento T-testo rezultatai lyginant vizualų ir nevizualų privatumo politikos pranešimų formatų įtaką veikiantį suvokiamą pasitikėjimą

Privatumo politikos pateikimo formatas	Imtis	Vidurkis	Standartinis nuokrypis	df	p	t
Vizualus formatas	245	4,5265	1,31778	488	0,000	5,200
Nevizualus formatas	245	3,9086	1,31279			

Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Trečiają hipotezę siekiama išsiaiškinti, ar suvokiama rizika yra veikiamas suvokiamas

pasitikėjimo. Atlikus Pearson koreliacijos duomenų analizę, **H3 yra priimta**, $R = -0,706$, $p < 0.001$ (žr. 10 lentelę). Suvokiamas pasitikėjimas veikia suvokiamą riziką priešingos krypties ryšiu.

10 lentelė

Suvokiamo pasitikėjimo ir suvokiamos rizikos koreliacija

		Suvokiamas pasitikėjimas	Suvokiama rizika
Suvokiamas pasitikėjimas	Pearson Correlation	1	-,706
	Sig. (1-tailed)		,000
	N	490	490
Suvokiama rizika	Pearson Correlation	-,706	1
	Sig. (1-tailed)	,000	
	N	490	490

Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Papildomai atlikus T testą, suvokiamas pasitikėjimas ($M = 4.2176$) vartotojams yra svarbesnis nei suvokiama rizika ($M = 3.7020$) $t(489) = -4,292$, $p < 0.001$ (žr. 11 lentelę). Išvados pritaria ir mokslininkai, teigdami, kad suvokiama rizika neigiamai koreliuoja su suvokiamu pasitikėjimu (Liao ir kt., 2011). Taip pat, jog suvokiamas pasitikėjimas sumažina rizikos suvokimą (Zimmer ir kt., 2010), todėl suvokiamo pasitikėjimo svarba tampa aukštesnė.

11 lentelė

Suvokiamo pasitikėjimo ir suvokiamos rizikos T- testo rezultatai

	Vidurkis	Standartinis nuokrypis	Stand. klaidos reikšmė	95% skirtumo pasitikėjimo intervalas		t	df	Sig. (2-tailed)
				apatinis	viršutinis			
Suvokiama rizika - pasitikėjimas	-0,51551	2,65901	0,12012	-0,75153	-0,27949	-4,292	489	0,000

Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Ketvirtąją hipotezę siekiama išsiaiškinti, suvokiamos rizikos daromą įtaką požiūriui į aplikaciją. Atlikus tiesinę regresiją, **H4 yra priimta**, bendruoju požiūriu, suvokiama rizika turi įtakos vartotojų požiūriui į aplikaciją $R^2 = 0.482$, $F(1) = 453,228$, $p < 0.001$ (žr. 7 priedą).

Remiantis Stjudento T-testo rezultatais, siekiant išsiaiškinti, kaip skirtingos rizikos (rizikingas ir nerizikingas) privatumo pranešimas veikia vartotojų požiūrį į aplikaciją, nustatyta, kad vartotojų požiūris yra labiau teigiamas, kai privatumo pranešimas yra įvardijamas nerizikingu ($M = 5,4184$)

lyginant su aukštesnės rizikos privatumo pranešimu ($M=4,0347$). Studento T-testo $t(483,549)=11,691$, $p<0.001$ (žr. 12 lentelę). Esantis žemas privatumo lygis mažina suvokiamą riziką (Lai ir kt., 2018). Suvokiama rizika duomenų apsauga neigiamai veikia požiūrį į aplikacijas (Lai ir kt., 2018). Todėl suvokiama rizika bei rizikos indikatoriai sąlygoja požiūrį į aplikacijas.

12 lentelė

Studento T-testo rezultatai lyginant vartotojų požiūrį į aplikaciją esant rizikingam ir nerizikingam privatumo pranešimui

Privatumo pranešimas	Imtis	Vidurkis	Standartinis nuokrypis	df	p	t
Rizikingas	245	4,0347	1,37130	483,549	0,000	11,691
Nerizikingas	245	5,4184	1,24547			

Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Penktąją hipotezę siekiama išsiaiškinti, suvokiamo pasitikėjimo daromą įtaką požiūriui į aplikaciją. Atlikus tiesinę regresiją, **H5 yra priimta**, suvokiamas pasitikėjimas turi įtakos vartotojų požiūriui į aplikaciją $R^2=0.576$, $F(1)=662,798$, $p<0.001$ (žr. 8 priedą). Su išvada sutinka ir kiti autoriai, teigdami, kad pasitikėjimas teigiamai veikia ketinimą naudotis aplikacijomis (Namara ir Knijnenburg, 2021) bei pozityviai veikia bendrąjį požiūrį į aplikacijas (Setiawan ir Widanta, 2021). Suvokiamas pasitikėjimas yra svarbus kintamasis ketinimo įsidiegti aplikacijas kontekste, nes pasitikėjimas padeda stiprinti požiūrį (Setiawan ir Widanta, 2021).

Šeštąją hipotezę siekiama išsiaiškinti, ar vartotojų amžius sąlygoja susidariusio požiūrio į aplikaciją įtaką ketinant ją įsidiegti. Atlikus moderaciją, **H6 yra atmesta**, duomenys rodo, jog amžius neturi moderacijos efekto susidariusiam požiūriui į aplikaciją ir ketinimui ją įsidiegti ($p>0,05$). Tačiau duomenys rodo, kad modelio reikšmingumas egzistuoja $R^2=0.5820$, $p<0.001$, taip pat susidaręs požiūris į aplikaciją turi tiesioginį poveikį ketinimui įsidiegti aplikaciją $p<0,001$ (žr. 9 priedą).

Septintąją hipotezę siekiama išsiaiškinti, ar vartotojų lytis sąlygoja susidariusio požiūrio į aplikaciją įtaką ketinant ją įsidiegti. Atlikus moderaciją, **H7 yra atmesta**, duomenys rodo, jog lytis neturi moderacijos efekto susidariusiam požiūriui į aplikaciją ir ketinimui ją įsidiegti ($p>0,05$). Tačiau duomenys rodo, kad modelio reikšmingumas egzistuoja $R^2=0.5818$, $p<0.001$. Kaip ir buvo patvirtinta H6, susidaręs požiūris į aplikaciją turi tiesioginį poveikį ketinimui ją įsidiegti $p<0,001$ (žr. 10 priedą). Hipotezė yra atmetama, tačiau nagrinėtuose šaltiniuose tarp tyrėjų taip pat vyravo išsiskiriančios nuomonės dėl lyties moderacijos efekto.

Aštuntąją hipotezę siekiama išsiaiškinti, ar aplikacijos kategorija sąlygoja susidariusio požiūrio į aplikaciją įtaką ketinant ją įsidiegti. Atlikus moderaciją, **H8 yra atmesta**, duomenys rodo, jog

aplikacijos kategorija (utilitarinė/hedoninė) moderacijos efekto susidariusiam požiūriui į aplikaciją ir ketinimui ją įsidiegti neturi ($p > 0,05$). Tačiau duomenys rodo, kad modelio reikšmingumas egzistuoja $R^2 = 0.5838$, $p < 0.001$. Kaip ir buvo patvirtinta H6 ir H7, susidaręs požiūris į aplikaciją turi tiesioginį poveikį ketinimui ją įsidiegti $p < 0,001$ (žr. 11 priedą). Priešiniai nei buvo tikėtasi, aplikacijos kategorija neturi moderacijos efekto tarp susidariusio požiūrio į aplikaciją ir ketinimo ją įsidiegti.

Devintąją hipotezę siekiama išsiaiškinti, ar ketinimas įsidiegti aplikacijas priklauso nuo susidariusio požiūrio į jas. Atlikus Pearson koreliacijos duomenų analizę, **H9 yra priimta**, kai $R = 0,762$, $p < 0.001$ (žr. 13 lentelę). Vartotojai įvertinę visas rizikas susiformuoja požiūrį į aplikacijas, teigiamas požiūris skatins vartotojus naudotis mobiliosiomis aplikacijomis (Belanche, Flavián ir Pérez-Rueda, 2020). Su hipotezės išvadomis sutinka ir kiti autoriai, teigdami, kad požiūris ir ketinimas įsidiegti mobiliąsias aplikacijas tarpusavyje koreliuoja (Zhang ir kt., 2018). Taip pat tyrimuose teigiama, jog bendras požiūris į aplikaciją teigiamai veikia vartotojų ketinimus (Sreejesh ir kt., 2016) ir sprendimų priėmimą (Tsai ir kt., 2011). Taip pat susidariusio požiūrio į aplikacijas ir ketinimo jas įsidiegti ryšys dar kartą buvo patvirtintas tikrinant H6 – H8 hipotezes.

13 lentelė

Požiūrio į aplikacijas ir ketinimo jas įsidiegti koreliacija

		Požiūris į aplikacijas	Ketinimas įsidiegti
Požiūris į aplikacijas	Pearson Correlation	1	,762
	Sig. (1-tailed)		,000
	N	490	490
Ketinimas įsidiegti	Pearson Correlation	,762	1
	Sig. (1-tailed)	,000	
	N	490	490

Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Taigi, atlikus surinktų duomenų analizę šešios iš devynių hipotezių pasitvirtino ir buvo priimtos (žr. 14 lentelę).

14 lentelė

Hipotezių rezultatai

Hipotezė	Rezultatai
H1: Privatumo politikos pranešimo formatų pateikimas teigiamai sąlygoja suvokiamą riziką	Priimta
H2: Privatumo politikos pranešimo formatų pateikimas teigiamai sąlygoja suvokiamą pasitikėjimą	Priimta
H3: Suvokiamas pasitikėjimas turi neigiamą ryšį su suvokiama rizika	Priimta
H4: Suvokiama rizika neigiamai sąlygoja požiūrį į aplikaciją	Priimta
H5: Suvokiamas pasitikėjimas sąlygoja požiūrį į aplikaciją	Priimta
H6: Amžius sąlygoja susidariusio požiūrio į aplikaciją įtaką ketinimui ją įsidiegti	Atmesta
H7: Lytis sąlygoja susidariusio požiūrio į aplikaciją įtaką ketinimui ją įsidiegti	Atmesta
H8: Aplikacijos kategorija sąlygoja susidariusio požiūrio į aplikaciją įtaką ketinimui ją įsidiegti	Atmesta
H9: Požiūris į aplikaciją teigiamai sąlygoja ketinimą ją įsidiegti	Priimta

Šaltinis: sudaryta darbo autorės

Priešingai nei buvo tikėtasi, lytis, amžius bei aplikacijos kategorija neturėjo įtakos susidariusio požiūrio į aplikacijas bei ketinimo jas įsidiegti ryšiui. Buvo nustatyta, jog šis ryšys veikia tiesiogiai. Tačiau skirtingai vaizduojamas privatumo politikos informacijos pateikimas turėjo įtakos suvokiamai rizikai ir pasitikėjimui, o šie kintamieji požiūriui į aplikaciją.

Vartotojai buvo linkę labiau atkreipti dėmesį į vizualiai pateiktas privatumo politikos nuostatas. Taip pat nustatyta, jog rizikingumo vaizdavimas teigiamai veikia suvokimą apie galimas rizikas. Respondentai buvo labiau linkę rinktis aplikacijas, kurių privatumo rizikos lygis buvo vaizduojamas kaip žemesnis. Bendrai, respondentams priimant sprendimą įsidiegti mobiliąsias aplikacijas tampa svarbiau suvokiamas pasitikėjimas nei suvokiama rizika.

Kitame skyriuje bus analizuojami pagrindinių situacijoms pasirinktų manipuliacijų ryšiai vienu metu.

3. 3. Pagrindinių situacijose naudotų manipuliacijos faktorių tarpusavio ryšių analizė

Nepriklausomai nuo iškeltų hipotezių, naudinga išsiaiškinti suvokiamą riziką, suvokiamą pasitikėjimą bei privatumo politikos pranešimo formatų svarbą esant skirtingiems aplikacijų tipams

(utilitarinei ir hedoninei) ir kitiems faktoriams, kaip privatumo politikos pranešimo rizikingumas, vienu metu. Šiais pagrindiniais faktoriais buvo siekiama manipuluoti pateiktas situacijas, todėl naudinga ištirti jų tarpusavio ryšius.

Pirmiausia, naudinga išanalizuoti, kaip buvo vertinama privatumo politikos pranešimo formatų svarba esant utilitarinei aplikacijai su vizualiu privatumo politikos nuostatų pateikimu bei hedoninei aplikacijai su nevizualiu privatumo politikos pateikimu. Atlikus faktorinę ANOVA, privatumo politikos pranešimo formatų svarba nuo aplikacijos tipo (utilitarinio/hedoninio) bei aplikacijos tipo ir privatumo politikos vizualikos iteracijos nesiskiria, nes $p > 0,05$, tačiau vertinimas skiriasi nuo paties privatumo politikos pranešimo formato (vizualaus/nevizualaus) (žr. 15 lentelę). Remiantis gautais duomenimis, vizualus privatumo politikos pranešimo formatas vartotojams buvo svarbesnis nepaisant skirtingo aplikacijos tipo (žr. 19 priedą).

15 lentelė

Faktorinė ANOVA vertinant privatumo politikos pranešimo formatų svarbą

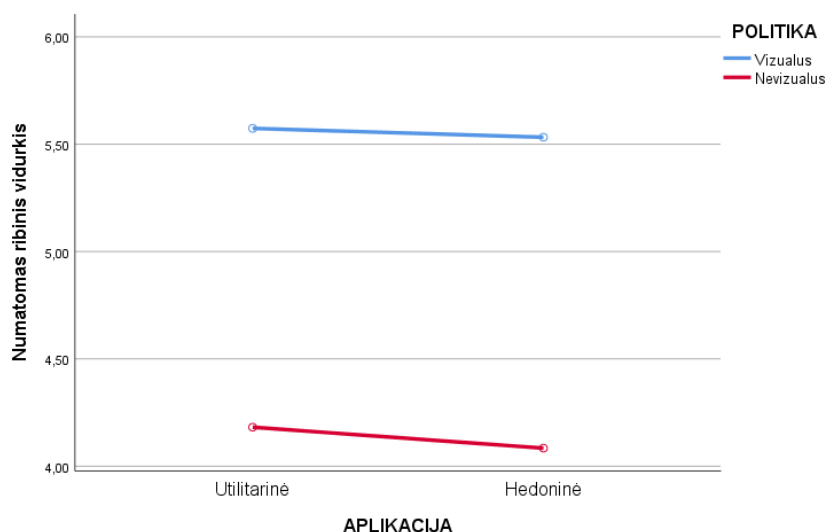
Kintamieji	df	Vidurkis	F	p
Aplikacijos kategorija	1	0,584	0,349	0,555
P. politikos pranešimo formatas	1	244,873	146,347	0,000
Aplikacijos kategorija X p. politikos pranešimo formatas	1	0,096	0,057	0,811

Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Rezultatai pabrėžia, kad utilitarinės aplikacijos su vizualiu privatumo politikos nuostatų pateikimu bei hedoninės aplikacijos su nevizualiu privatumo politikos nuostatų pateikimu iteracijos vidurkiai skiriasi (žr. 5 paveikslą).

5 paveikslas

Aplikacijos tipo ir privatumo politikos nuostatų pateikimo iteracija



Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Antra, faktorinės ANOVA analizės rezultatai rodo, kad hedoninės aplikacijos su vizualių privatumo politikos nuostatų pateikimu bei utilitarinės aplikacijos su nevizualių privatumo politikos pateikimu vidurkiai taip pat skiriasi.

Taip pat buvo analizuojama, kaip vertinama suvokiama rizika esant pateiktam skirtingam privatumo pranešimo rizikingumo lygiui ir aplikacijos tipui. Lyginama utilitarinė aplikacija su rizikingu privatumo politikos nuostatų pateikimu bei hedoninė aplikacija su nerizikingu privatumo politikos pateikimu. Nustatyta, kad suvokiama rizika nuo aplikacijos tipo ir aplikacijos tipo bei privatumo pranešimo rizikingumo pateikties iteracijos nesiskiria, nes $p > 0,05$. Tačiau suvokiama rizika skiriasi nuo skirtingos privatumo pranešimo rizikingumo pateikties (rizikingas/nerizikingas), $p < 0,01$ (žr. 16 lentelę).

16 lentelė

Faktorinė ANOVA vertinant suvokiamos rizikos svarbą

Kintamieji	df	Vidurkis	F	p
Aplikacijos kategorija	1	0,349	0,189	0,664
Privatumo pranešimo rizikingumo lygmuo	1	245,322	132,950	0,000
Aplikacijos kategorija X privatumo pranešimo rizikingumo lygmuo	1	0,018	0,009	0,922

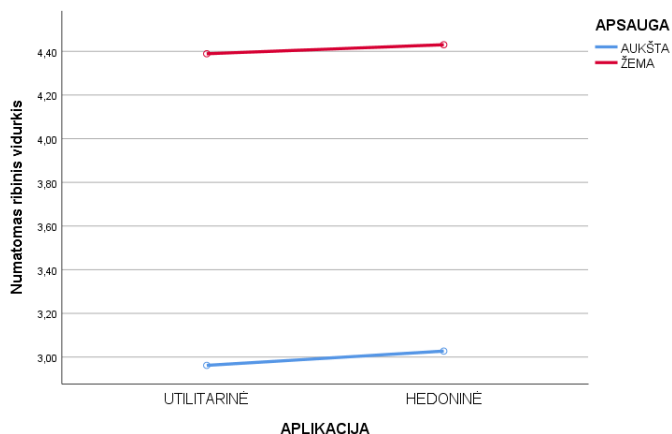
Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Rezultatai pabrėžia, kad utilitarinės aplikacijos su rizikingu privatumo politikos nuostatų pateikimu bei hedoninės aplikacijos su nerizikingu privatumo politikos pateikimu iteracijos vidurkiai skiriasi. Taip pat utilitarinės aplikacijos su nerizikingu privatumo politikos nuostatų pateikimu bei

hedoninės aplikacijos su rizikingu privatumo politikos pateikimu vidurkiai skiriasi (žr. 6 paveikslą).

6 paveikslas

Aplikacijos tipo ir privatumo pranešimo rizikingumo lygmens iteracija



Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Remiantis gautais duomenimis, suvokiamos rizika, nepaisant skirtingo aplikacijos tipo, buvo aukštesnė, kai privatumo pranešimo rizikingumo lygmuo buvo aukštas (žr. 20 priedą).

Atlikus faktorinę ANOVA, siekiant nustatyti, kaip vertinamas suvokiamas pasitikėjimas esant pateiktam skirtingam privatumo pranešimo rizikingumo lygiui ir aplikacijos tipui. Lyginama utilitarinė aplikacija su rizikingu privatumo politikos nuostatų pateikimu bei hedoninė aplikacija su nerizikingu privatumo politikos pateikimu. Nustatyta, kad suvokiamas pasitikėjimas nuo aplikacijos tipo ir aplikacijos tipo bei privatumo pranešimo rizikingumo pateikties iteracijos nesiskiria, nes $p > 0,05$. Tačiau suvokiamo pasitikėjimo svarba skiriasi nuo skirtingos privatumo pranešimo rizikingumo pateikties (rizikingas/nerizikingas), $p < 0,01$ (žr. 17 lentelę).

17 lentelė

Faktorinė ANOVA vertinant suvokiamo pasitikėjimo svarbą

Kintamieji	df	Vidurkis	F	p
Aplikacijos kategorija	1	1,438	0,957	0,328
Privatumo pranešimo rizikingumo lygmuo	1	159,436	106,136	0,000
Aplikacijos kategorija X privatumo pranešimo rizikingumo lygmuo	1	0,197	0,131	0,717

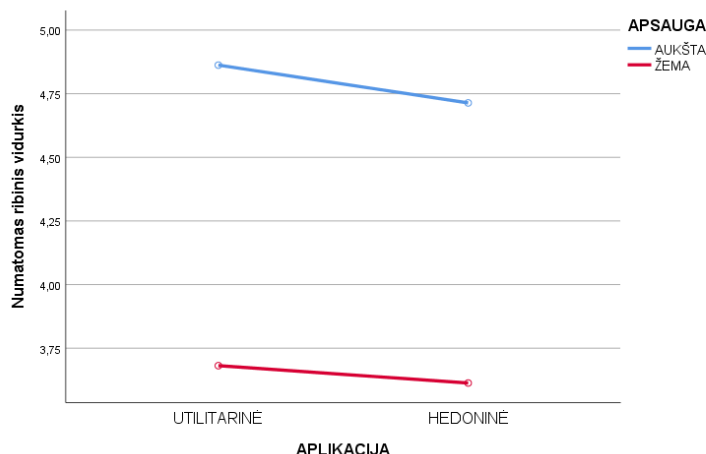
Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Rezultatai pabrėžia, kad utilitarinės aplikacijos su rizikingu privatumo politikos nuostatų pateikimu bei hedoninės aplikacijos su nerizikingu privatumo politikos pateikimu iteracijos vidurkiai skiriasi. Taip pat utilitarinės aplikacijos su nerizikingu privatumo politikos nuostatų pateikimu bei hedoninės aplikacijos su rizikingu privatumo politikos pateikimu vidurkiai skiriasi (žr. 7 paveikslą).

Remiantis gautais rezultatais, suvokiamas pasitikėjimas nepaisant skirtingo aplikacijos tipo buvo aukštesnis, kai privatumo pranešimo rizikingumo lygmuo buvo žemas (žr. 21 priedą).

7 paveikslas

Aplikacijos tipo ir privatumo pranešimo rizikingumo lygmens iteracija



Šaltinis: sudaryta autorės, remiantis IBM SPSS analizės rezultatais

Taigi, atlikus papildomą faktoriinę ANOVA analizę nustatyta, kad privatumo politikos pranešimo formatų svarbos vertinimas skiriasi nuo vizualinio pateikimo (vizualaus/nevizualaus). Tačiau privatumo politikos pranešimo formatų svarbos vertinimas nuo aplikacijos tipo (utilitarinio/hedoninio) bei aplikacijos tipo ir privatumo politikos vizualikos iteracijos nesiskyrė. Suvokiama rizika kaip ir suvokimas pasitikėjimas nuo aplikacijos tipo ir aplikacijos tipo bei privatumo pranešimo rizikingumo pateikties iteracijos nesiskyrė. Tačiau tyrimo rezultatai parodė, kad suvokiama rizika ir suvokiamas pasitikėjimas skiriasi nuo skirtingos privatumo pranešimo rizikingumo pateikties (rizikingas/nerizikingas).

Kitame skyriuje bus įvardijami baigiamojo darbo tyrimo ribotumai.

3. 4. Tyrimo ribotumai

Pirmiausia, tyrimui pasirinkta neatsitiktinė patogioji atranka, todėl tyrimo rezultatai negali būti pritaikomi visai populiacijai. Tyrimas buvo atliekamas lietuvių kalba, todėl ne visiems respondentams tyrimo anketa galėjo pritaikoma. Nors tyrimui išankstinės tautybės ar amžiaus kategorijos nebuvo taikomos.

Tyrimo buvo pasirinkta tirti tik dvi skirtingas mobiliųjų aplikacijų kategorijas: socialinių tinklų ir kasdieninių finansų. Esant kitoms mobiliųjų aplikacijų kategorijoms rezultatai gali kisti. Taip pat pasirinktos aplikacijos nebuvo egzistuojančios, todėl respondentai pildydami apklausą nedalyvavo

eksperimente, suvokiamos rizikos galėjo būti žemesnės, nes nebuvo stimulo ir reakcijos dėl realios rizikos. Be to, sudarant tyrimo situacijas remtasi kitų mokslininkų duomenimis anglų kalba, todėl galėjo pasitaikyti vertinimo ir sąvokų interpretavimo klaidų.

Tyrimo rezultatams surinkti, situacijose buvo pateikiamos privatumo politikos ištraukos. Respondentai galėjo turėti išankstinę nuomonę iš realios patirties apie privatumo pranešimus ar jų naudą bei tikslą, todėl bendras požiūris į hipotetines situacijas galėjo būti veikiamas realios patirties išankstinių nuostatų.

Tyrimo rezultatuose lytis, amžius bei aplikacijos kategorija, priešingai nei mokslinėje literatūroje, neturėjo įtakos tam tikriems modelyje analizuojamiems ryšiams, todėl rezultatai galėtų būti skirtingi, jei šie kintamieji veiktų kitus modelyje analizuojamus ryšius.

IŠVADOS IR PASIŪLYMAI

1) Remiantis literatūros analize, privatumo politikos įstatymai leidžia apsaugoti vartotojus nuo duomenų nutekimo, grubių asmens duomenų pažeidimų. Teisingas privatumo politikos nuostatų pateikimas turi būti siejamas su tikslumu, teisėtumu, vientisumu ir konfidencialumu, tikslo apribojimais, duomenų minimizavimu bei saugumo apribojimais. Kuriant mobiliąsias aplikacijas bei įvedant privatumo politikos nuostatus, svarbiausia įgyvendinti pakankamą vartotojų informavimą, visada renkant duomenis turi būti įvardijamas jų tikslas, kontaktinė informacija, suteikianti vartotojams galimybę kreiptis dėl savo duomenų. Vartotojams privalo būti suteikiama kontrolė valdyti savo asmeninę informaciją, atsisakyti pateikti tam tikrus duomenis bei teisė būti pamirštam. Bendrai, įmonės privalo užtikrinti bei laikytis duomenų apsaugos principų.

2) Ketinimui įsdiegti mobiliąsias aplikacijas įtakos turi vartotojų suvokiamas aplikacijų naudingumas bei vertės. Moksliniuose šaltiniuose pagrindinės vertės įvardijamos kaip: hedoninės, utilitarinės, socialinės ir episteminės. Jos siejamos su vartotojų džiaugsmu ir patyrimais, naudingumu ir informacijos pakankamumu, siekiu kuri įvaizdį kitų akyse ar kurti socialinę gerovę bei vartotojų noras išbandyti naujoves ir technologijas. Taip pat vertės gali būti suvokiamos esant skirtingoms aplikacijų charakteristikoms, kaip atsiliepimais, aplikacijos įsdiegimo rodikliu, reitingu. Literatūros analizėje pabrėžiama, kad suvokiamas aplikacijų naudingumas yra siejamas su galimomis rizikomis ir požiūriu į jas. Moksliniuose tyrimuose daugiausiai duomenų apsaugos reikalaujančiomis aplikacijos išskiriamos mobiliosios bankininkystės aplikacijos. Prieštaringos nuomonės buvo laikomasi tiriant hedoninės, dažniausiai socialinių tinklų ar pramogines aplikacijas. Jos taip pat įvardijamos kaip daugiausia privatumo pažeidimų sukeliančios aplikacijos, nors skirtingi tyrėjai šiam teiginiui turėjo skirtingas išvadas ir nuomonę.

3) Mokslinėje literatūroje suvokiama rizika bei suvokiamas pasitikėjimas įvardijami kaip tarpusavyje veikiantys kintamieji. Darbe nustatyta, kad suvokiamas pasitikėjimas veikia suvokiamą riziką priešingos krypties ryšiu. Pirmiausia, suvokiamą riziką ir pasitikėjimą veikia pačių vartotojų susirūpinimas savo duomenų saugumu. Susirūpinimas gali būti aukštas arba žemas. Darbe nustatyta, kad suvokiamas pasitikėjimas vartotojams yra svarbesnis nei suvokiama rizika. Remiantis mokslinė analize ir darbe sudarytu tyrimo modeliu bei tyrimo rezultatais, suvokiama rizika ir pasitikėjimas pirmiausia sudaro bendrą požiūrį į aplikacijas. Nustatyta, jog suvokiama rizika ir suvokiamas pasitikėjimas turi įtakos vartotojų požiūriui į aplikacijas. Pasitikėjimas yra teigiamą poveikį ketinimui įsdiegti aplikacijas turintis kintamasis, nes jis padeda stiprinti požiūrį. Be to, nustatyta, kad suvokiamos rizikos ir pasitikėjimo sudarytas bendras požiūris į aplikacijas tarpusavyje koreliuoja su ketinimu įsdiegti mobiliąsias aplikacijas. Remiantis išvadomis, komunikacija apie galimas rizikas turėtų būti pateikiama kaip galima anksčiau prieš įsdiegiant aplikacijas. Pasak mokslinių šaltinių, dažniausiai rizikos gali būti komunikuojamos pasitelkiant grafinį rizikingumo vaizdavimą, kuris taip pat padeda

įvertinti pačias rizikas.

4) Mokslinėje literatūroje teigiama, kad vartotojai yra linkę atkreipti dėmesį į aiškiai aprašytus privatumo politikos nuostatus nei į minimaliai ar visai nepateiktus nuostatus. Vartotojai linkę labiau įsitraukti ir susipažinti su privatumo praktikomis, kai informacija apie jas yra pateikiama kartu privatumo lygmenį vaizduojančiomis ikonomis. Nagrinėtoje literatūroje šis duomenų vaizdavimas įvardijamas kaip reikšmingas veiksnys aplikacijų pasirinkimui. Be to, grafinis privatumo politikos pranešimo vaizdavimas taupo laiką, edukuoja ir įspėja vartotoją apie galimas grėsmes. Tačiau praktikoje privatumo politikos nuostatai yra išdėstomi tik tekstiniu būdu. Anot nagrinėtų mokslininkų tyrimų išvadų, tekstinis išdėstymas yra komplikotas, vartotojams sunkiai perprantamas, ypač, kai ne visi vartotojai gali vienodai suprasti teisinę kalbą, ar jų elgesys duomenų saugumo atžvilgiu gali būti žemas. Todėl mokslinėje literatūroje grafinis privatumo politikos pranešimo pateikimas įvardijamas kaip vienas iš geriausių būdų, atitinkančių BDAR reikalavimus.

5) Darbe atlikto tyrimo išvados nurodo, kad suvokiama rizika skiriasi nuo skirtingos privatumo pranešimo rizikingumo pateikties. Taip pat tyrimo rezultatai patvirtina, kad vartotojų požiūris yra labiau teigiamas, kai privatumo pranešimas yra įvardijamas nerizikingu lyginant su aukštesnės rizikos privatumo pranešimu. Bendrai privatumo politikos pranešimo formatų svarbos vertinimas skiriasi nuo vizualinio pateikimo (vizualaus/nevizualaus). Vizualus privatumo politikos pranešimo formatas vartotojams buvo svarbesnis lyginant su nevizualia pateiktimi nepaisant skirtingo aplikacijos tipo. Vartotojų suvokiama rizika buvo didesnė, kai yra pateikiamas nevizualus privatumo politikos pranešimo formatas lyginant su vizualiu. Tačiau privatumo politikos pranešimo formatų svarbos vertinimas nuo aplikacijos tipo (utilitarinio/hedoninio) bei aplikacijos tipo ir privatumo politikos vizualikos iteracijos nesiskyrė. Suvokiama rizika kaip ir suvokimas pasitikėjimas nuo aplikacijos tipo ir aplikacijos tipo bei privatumo pranešimo rizikingumo pateikties iteracijos nesiskyrė. Tačiau tyrimo rezultatai parodė, kad suvokiama rizika ir suvokiamas pasitikėjimas skiriasi nuo skirtingos privatumo pranešimo rizikingumo pateikties (rizikingas/nerizikingas). Suvokiama rizika, nepaisant skirtingo aplikacijos tipo, buvo aukštesnė, kai privatumo pranešimo rizikingumo lygmuo buvo aukštas. Gauti rezultatai nurodo, kad suvokiamas pasitikėjimas, nepaisant skirtingo aplikacijos tipo, buvo aukštesnis, kai privatumo pranešimo rizikingumo lygmuo buvo žemas. Tačiau priešingai nei buvo tikėtasi, tirti demografiniai duomenys, tokie kaip amžius ir lytis, neturėjo sąveikos susidariusio požiūrio į aplikacijas įtakai ketinimui jas įsidiegti. Kaip ir skirtinga aplikacijos kategorija.

Remiantis mokslinės literatūros analize ir gautais tyrimo duomenimis, pateikiamos rekomendacijos tolimesniems tyrimams bei pasiūlymai verslui:

1. Ateities tyrimuose būtų naudinga tirti konkrečias rizikas (pvz.: piniginiai nuostoliai, pavojus įrenginiui, t.t.). Šiame darbe konkreti rizika nebuvo įvardijama.
2. Darbe buvo tiriamos socialinių tinklų ir kasdieninių finansų aplikacijos. Tolimesniuose

tyrimuose būtų naudinga tirti kitas aplikacijų kategorijas. Skirtingos aplikacijų kategorijos galimai galėtų paveikti rezultatus.

3. Remiantis darbo ribotumais, būtų naudinga apjungti kokybinius ir kiekybinius tyrimo metodus išsamesniems rezultatams gauti.

Pasiūlymai verslui:

1. Sudarant privatumo politikos nuostatus, naudinga juos pateikti grafiškai kartu su rizikingumo lygmenį vaizduojančiomis ikonomis. Remiantis gautomis išvadomis, pateikiant privatumo pranešimą, patartina vengti tik tekstinio išdėstymo. Kadangi vizuali pateiktis vartotojams buvo svarbesnė ir labiau atkreipianti dėmesį nepriklausomai nuo aplikacijos kategorijos, vartotojų lyties ir amžiaus. Todėl grafinis rizikingumo vaizdavimas galėtų būti pritaikomas visoms aplikacijos nepaisant kategorijos.

2. Privatumo politikos nuostatos turi būti aiškios ir konkrečios, kad rizikingumo lygmenį vaizduojančios ikonos būtų veiksmingos. Tokiu būdu suvokiama rizika nebus didesnė nei suvokiamas aplikacijos naudingumas. Be to, bus laikomasi pagrindinių BDAR principų. Remiantis tyrimo rezultatais, sudarytas teigiamas požiūris į aplikacijas turi tiesioginį poveikį ketinimui jas įsidiesti.

3. Kadangi tyrimo rezultatais patvirtinta, kad vizualizaciniai privatumo politikos pateikimo formatai veikia vartotojų suvokiamas rizikas ir pasitikėjimą, verslui naudinga pradėti naudoti vizualizacinius sprendimus kuriant ar jau sukūrus mobiliąsias aplikacijas. Tokiu būdu bus išsiskiriama iš konkurencinės aplinkos.

LITERATŪROS IR ŠALTINIŲ SĄRAŠAS

- Aïmeur, E., Gambs, S., & Ho, A. (2009). *UPP: User Privacy Policy for Social Networking Sites*. 2009 Fourth International Conference on Internet and Web Applications and Services. doi:10.1109/iciw.2009.45
- Aïmeur, E., Lawani, O., & Dalkir, K. (2016). *When changing the look of privacy policies affects user trust: An experimental study*. *Computers in Human Behavior*, 58, 368–379. doi:10.1016/j.chb.2015.11.014
- Ajzen, I. (1991). *The theory of planned behavior*. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. doi:10.1016/0749-5978(91)90020-t
- Aleem, U., Cavusoglu, H. ir Benbasat, I. (2017). *An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps*. Sauder School of Business, University of British Columbia. DOI:10.1287/isre.2020.0931
- Ali, M., Joorabchi, M. E. ir Mesbah, A. (2017). *Same App, Different App Stores: A Comparative Study*. 2017 IEEE/ACM 4th International Conference on Mobile Software Engineering and Systems (MOBILESoft). doi:10.1109/mobilesoft.2017.3
- Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). *Mobile application security: Role of perceived privacy as the predictor of security perceptions*. *International Journal of Information Management*, 102063. doi:10.1016/j.ijinfomgt.2019.102063
- Bansal, G., Zahedi, F. M. ir Gefen, D. (2008). *The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation*. ICIS 2008 Proceedings. Paper 7. Prieiga internetu: <http://aisel.aisnet.org/icis2008/7>
- Bansal, G., Zahedi, F. M. ir Gefen, D. (2015). *The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern*. *European Journal of Information Systems*, 24(6), 624–644. doi:10.1057/ejis.2014.41
- Belanche, D., Flavián, M. ir Pérez-Rueda, A. (2020). *Mobile Apps Use and WOM in the Food Delivery Sector: The Role of Planned Behavior, Perceived Security and Customer Lifestyle Compatibility*. *Sustainability*, 12(10), 4275. doi:10.3390/su12104275
- Bergström, A. (2015). *Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses*. *Computers in Human Behavior*, 53, 419–426. doi:10.1016/j.chb.2015.07.025
- Betzing, J. H., Tietz, M., vom Brocke, J. ir Becker, J. (2019). *The impact of transparency on mobile privacy decision making*. *Electronic Markets*. doi:10.1007/s12525-019-00332-3

Bilevičienė, T. ir Jonušauskas, S. (2011). *STATISTINIŲ METODŲ TAIKYMAS RINKOS TYRIMUOSE*. Vilnius: Mykolo Romerio universiteto Leidybos centras

Brandtzaeg, P. B., Pultier, A. ir Moen, G. M. (2018). *Losing Control to Data-Hungry Apps*. *Social Science Computer Review*, 37(4), 466–488. <https://doi.org/10.1177/0894439318777706>

Chang, Y., Wong, S. F., Libaque-Saenz, C. F. ir Lee, H. (2018). *The role of privacy policy on consumers' perceived privacy*. *Government Information Quarterly*, 35(3), 445–459. doi:10.1016/j.giq.2018.04.002

Cheng, E. W. L. (2018). *Choosing between the theory of planned behavior (TPB) and the technology acceptance model (TAM)*. *Educational Technology Research and Development*. doi:10.1007/s11423-018-9598-6

Chen, Y., Yan, X., Fan, W., & Gordon, M. (2015). *The joint moderating role of trust propensity and gender on consumers' online shopping behavior*. *Computers in Human Behavior*, 43, 272–283. doi:10.1016/j.chb.2014.10.020

Chen, J. (2020). *Risk Communication in Cyberspace: A Brief Review of The Information-Processing and Mental Models Approaches*. *Current Opinion in Psychology*. doi:10.1016/j.copsyc.2020.06.006

Chen, J., Gates, C. S., Li, N. ir Proctor, R. W. (2015). *Influence of Risk/Safety Information Framing on Android App-Installation Decisions*. *Journal of Cognitive Engineering and Decision Making*, 9(2), 149–168. doi:10.1177/1555343415570055

Chen, J., Ge, H., Moore, S., Yang, W., Li, N. ir Proctor, R. W. (2018). *Display of major risk categories for android apps*. *Journal of Experimental Psychology: Applied*, 24(3), 306–330. <https://doi.org/10.1037/xap0000163>

Chin, A. G., Harris, M. A. ir Brookshire, R. (2018). *A bidirectional perspective of trust and risk in determining factors that influence mobile app installation*. *International Journal of Information Management*, 39, 49–59. doi:10.1016/j.ijinfomgt.2017.11.010

Chin, E., Felt, A. P., Sekar, V. ir Wagner, D. (2012). *Measuring user confidence in smartphone security and privacy*. *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*. doi:10.1145/2335356.2335358

Choi, B. C. F. ir Land, L. (2016). *The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage*. *Information & Management*, 53(7), 868–877. doi:10.1016/j.im.2016.02.003

Choi, T. R. ir Sung, Y. (2018). *Instagram versus Snapchat: Self-expression and privacy concern on social media*. *Telematics and Informatics*. doi:10.1016/j.tele.2018.09.009

Chong, I., Ge, H., Li, N. ir Proctor, R. W. (2018). *Influence of privacy priming and security framing on mobile app selection*. *Computers & Security*, 78, 143–154.

doi:10.1016/j.cose.2018.06.005

Crossler, R. E. ir Bélanger, F. (2017). *The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors*. Proceedings of the 50th Hawaii International Conference on System Sciences. doi:10.24251/HICSS.2017.491

Davis, F. D. (1989). *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*. MIS Quarterly, 13(3), 319. doi:10.2307/249008

Dimodugno, M., Hallman, S., Plaisent, M. ir Bernard, P. (2021). *The effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information: A game theory-based approach*. In Journal of Physics: Conference Series 2090(1). doi:10.1088/1742-6596/2090/1/012017

Europos komisija. Kas yra asmens duomenys? Prieiga internetu: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_lt (Žiūrėta 2020-07-22)

European Parliament. Understanding EU data protection policy. Prieiga internetu: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651923/EPRS_BRI\(2020\)651923_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651923/EPRS_BRI(2020)651923_EN.pdf) (Žiūrėta 2020-07-22)

Ermakova, T., Baumann, A., Fabian, B. ir Krasnova, H. (2014). *Privacy policies and users' trust: does readability matter?*. In Twentieth americas conference on information systems, Georgia (pp. 1e12). DOI:10.7892/BORIS.68895

Esteve, A. (2017). *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA*. International Data Privacy Law, 7(1), 36–47. doi:10.1093/idpl/ipw026

Faqih, K. M. S. (2016). *An empirical analysis of factors predicting the behavioral intention to adopt Internet shopping technology among non-shoppers in a developing country context: Does gender matter?* Journal of Retailing and Consumer Services, 30, 140–164. doi:10.1016/j.jretconser.2016.01.016

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E. ir Wagner, D. (2012). *Android permissions: User Attention, Comprehension, and Behavior*. Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12. doi:10.1145/2335356.2335360

Flavián, C. ir Guinalíu, M. (2006). *Consumer trust, perceived security and privacy policy*. Industrial Management & Data Systems, 106(5), 601–620. doi:10.1108/02635570610666403

Flora, H., Wang, X. ir Chande, S.V. (2014). *An Investigation on the Characteristics of Mobile Applications: A Survey Study*. International Journal of Information Technology and Computer Science, 6, 21-27. doi: 10.5815/ijitcs.2014.11.03

Fong, L. H. N., Lam, L. W. ir Law, R. (2017). *How locus of control shapes intention to reuse mobile apps for making hotel reservations: Evidence from chinese consumers*. Tourism

Management, 61, 331–342. doi:10.1016/j.tourman.2017.03.002

Gaižauskaitė, I. ir Mikėnė, S. (2014). *SOCIALINIŲ TYRIMŲ METODAI: APKLAUSA*. Vilnius: Mykolo Romerio universitetas

Gates, C. S., Chen, J., Li, N. ir Proctor, R. W. (2014). *Effective Risk Communication for Android Apps*. IEEE Transactions on Dependable and Secure Computing, 11(3), 252–265. doi:10.1109/tdsc.2013.58

Ghazinour, K. ir Albalawi, T. (2016). *A Usability Study on the Privacy Policy Visualization Model*. 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech). doi:10.1109/dasc-picom-datacom-cyberscitech.2016.109

Giampietri, E., Verneau, F., Del Giudice, T., Carfora, V. ir Finco, A. (2018). *A Theory of Planned behaviour perspective for investigating the role of trust in consumer purchasing decision related to short food supply chains*. Food Quality and Preference, 64, 160–166. doi:10.1016/j.foodqual.2017.09.012

Gimpel, H., Kleindienst, D., Nüske, N., Rau, D. ir Schmied, F. (2018). *The upside of data privacy – delighting customers by implementing data privacy measures*. Electronic Markets. doi:10.1007/s12525-018-0296-3

Gu, J., Xu, Y. (Calvin), Xu, H., Zhang, C. ir Ling, H. (2016). *Privacy concerns for mobile app download: An elaboration likelihood model perspective*. Decision Support Systems, 94, 19–28. doi:10.1016/j.dss.2016.10.002

Haggag, O., Haggag, S., Grundy, J. ir Abdelrazek, M. (2021). *COVID-19 vs Social Media Apps: Does Privacy Really Matter?* 2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS). doi:10.1109/icse-seis52602.2021.00014

Hammouri, Q., Almajali, D. A., Nusairat, N. M. ir Saraireh, S. A. M. (2020). *Determinants of Users' Satisfaction with Mobile Apps*. International Journal of Advanced Science and Technology, 29(3), 14613 – 14624. Prieiga internetu: <http://sersc.org/journals/index.php/IJAST/article/view/31949>

Harris, M. A., Brookshire, R. ir Chin, A. G. (2016). *Identifying factors influencing consumers' intent to install mobile applications*. International Journal of Information Management, 36(3), 441–450. doi:10.1016/j.ijinfomgt

Harris, M. A., Brookshire, R., Patten, K. P. ir Regan, E. A. (2015a). *Mobile application installation influences: Have mobile device users become desensitized to excessive permission*

requests? In 2015 Americas Conference on Information Systems, AMCIS 2015 (2015 Americas Conference on Information Systems, AMCIS 2015). Americas Conference on Information Systems. Prieiga internetu: <https://bit.ly/3J3fpdB> (Žiūrėta 2020-07-22)

Harris, M. A., Chin, A. G. ir Brookshire, R. (2015b). *Mobile App Installation: the Role of Precautions and Desensitization*. Journal of International Technology and Information Management, 24(4), Article 3. Prieiga internetu: <http://scholarworks.lib.csusb.edu/jitim/vol24/iss4/3> (Žiūrėta 2020-07-22)

Harris, M. A. ir Chin, A. G. (2016). *Consumer trust in Google's top developers' apps: an exploratory study*. Information and Computer Security, 24(5), 474–495. doi:10.1108/ics-11-2015-0044

Hassandoust, F., Akhlaghpour, S. ir Johnston, A. C. (2020). *Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective*. Journal of the American Medical Informatics Association. doi:10.1093/jamia/ocaa240

Hatamian, M., Serna, J. ir Rannenberg, K. (2019). *Revealing the Unrevealed: Mining Smartphone Users Privacy Perception on App Markets*. Computers & Security. doi:10.1016/j.cose.2019.02.010

Hong, W. ir Thong, J. Y. L. (2013). *Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies*. MIS Quarterly, 37(1), 275–298. doi:10.25300/misq/2013/37.1.12

Hossain, M. A. (2019). *Security perception in the adoption of mobile payment and the moderating effect of gender*. PSU Research Review, 3(3), 179–190. doi:10.1108/prr-03-2019-0006

Hur, H. J., Lee, H. K. ir Choo, H. J. (2017). *Understanding usage intention in innovative mobile app service: Comparison between millennial and mature consumers*. Computers in Human Behavior, 73, 353–361. doi:10.1016/j.chb.2017.03.051

Ismail, Q., Ahmed, T., Kapadia, A. ir Reiter, M. K. (2015). *Crowdsourced Exploration of Security Configurations*. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15. doi:10.1145/2702123.2702370

Yan, Z., Liu, C., Niemi, V. ir Yu, G. (2013). *Exploring the impact of trust information visualization on mobile application usage*. Personal and Ubiquitous Computing, 17(6), 1295–1313. doi:10.1007/s00779-013-0636-4

Jones, R., Sailaja, N. ir Kerlin, L. (2017). *Probing the Design Space of Usable Privacy Policies: A Qualitative Exploration of a Reimagined Privacy Policy and Data Exchange Model*. 1-12. Doi: 10.14236/ewic/HCI2017.50.

Keith, M. J., Babb, J., Furner, C., Abdullat, A. ir Lowry, P. (2016). *Limited Information and Quick Decisions: Consumer Privacy Calculus for Mobile Applications*. AIS Transactions on Human-Computer Interaction, 8(3), 88-130. DOI:10.17705/1thci.00081

Kelley, P. G., Cranor, L. F. ir Sadeh, N. (2013). *Privacy as part of the app decision-making process*. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13. doi:10.1145/2470654.2466466

Kerviler, G., D., Demoulin, N. T. M. ir Zidda, P. (2016). *Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers?* Journal of Retailing and Consumer Services, 31, 334–344. doi:10.1016/j.jretconser.2016.04.011

Kim, D. J., Ferrin, D. L. ir Rao, H. R. (2008). *A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents*. Decision Support Systems, 44(2), 544–564. doi:10.1016/j.dss.2007.07.001

Kim, S. C., Yoon, D. ir Han, E. K. (2014). *Antecedents of mobile app usage among smartphone users*. Journal of Marketing Communications, 22(6), 653–670. doi:10.1080/13527266.2014.951065

Kitkowska, A., Warner, M., Shulman, Y., Wästlund, E. ir Martucci, L. (2020). *Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affe In: Proceedings of the Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. doi.org/10.5281/zenodo.3980478

Krafft, M., Arden, C. M. ir Verhoef, P. C. (2017). *Permission Marketing and Privacy Concerns — Why Do Customers (Not) Grant Permissions?* Journal of Interactive Marketing, 39, 39–54. doi:10.1016/j.intmar.2017.03.001

Kristadi, D. ir Sucahyo, Y. G. (2016). *Factors analysis of IPv6 user acceptance against security aspects based on concept of technology acceptance model (TAM) and technology threat avoidance theory (TTAT)*. 2016 International Conference on Advanced Computer Science and Information Systems (ICACSIS), Malang, 67-72, doi: 10.1109/ICACSIS.2016.7872750.

Kumaraguru, P ir Cranor, L. F. (2005). *Privacy Indexes: A Survey of Westin's Studies (CMU-ISRI-5-138)*. Institute for Software Research International, School of Computer Science, Carnegie Mellon University. Prieiga internetu: <https://bit.ly/3mkP4hp> (Žiūrėta 2020-07-22)

Kununka, S., Mehandjiev, N. ir Sampaio, P. (2018). *A Comparative Study of Android and iOS Mobile Applications' Data Handling Practices Versus Compliance to Privacy Policy*. Privacy and Identity Management. The Smart Revolution, 301–313. doi:10.1007/978-3-319-92925-5_20

Lai, H., Hsu, J. ir Wu, M. X. (2018). *The Impact s of Requested Permission on Mobile App Adoption: The Insights Based on an Experiment in Taiwan*. 10.24251/HICSS.2018.490.

Liao, C., Liu, C.C. ir Chen, K. (2011). *Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model*. Electronic Commerce Research and Applications, 10(6), 702–715. doi:10.1016/j.elerap.2011.07.003

Limba, T., Driaunys, K., Kiskis, M., Sidlauskas, A. (2020). *Development of Digital Contents: Privacy Policy Model under the General Data Protection Regulation and User-Friendly Interface*. Transformations in Business & Economics, 19(1), (49), 133- 154. Prieiga internetu: <http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=84afd148-f811-4470-81c5-f403f86b441e%40sessionmgr4008> (Žiūrėta 2020-07-22)

Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J. I. ir Zhang, J. (2012). *Expectation and purpose*. Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12. doi:10.1145/2370216.2370290

Lwin, M. O., Wirtz, J. ir Stanaland, A. J. S. (2016). *The privacy dyad*. Internet Research, 26(4), 919–941. doi:10.1108/intr-05-2014-0134

Malik, A., Suresh, S. ir Sharma, S. (2017). *Factors influencing consumers' attitude towards adoption and continuous use of mobile applications: a conceptual model*. Procedia Computer Science, 122, 106–113. doi:10.1016/j.procs.2017.11.348

Martin, K. D., Borah, A. ir Palmatier, R. W. (2017). *Data Privacy: Effects on Customer and Firm Performance*. Journal of Marketing, 81(1), 36–58. doi:10.1509/jm.15.0497

Martin, K. D. ir Murphy, P. E. (2016). *The role of data privacy in marketing*. Journal of the Academy of Marketing Science, 45(2), 135–155. doi:10.1007/s11747-016-0495-4

Martin, K. ir Shilton, K. (2016). *Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices*. The Information Society, 32(3), 200-216. DOI: 10.1080/01972243.2016.1153012

Meier, Y., Schäwel, J. ir Krämer, N. (2020). *The Shorter the Better? Effects of Privacy Policy Length on Online Privacy Decision-Making*. Media and Communication. 8(2), 291-301. DOI: 10.17645/mac.v8i2.2846.

Meinert, D. B., Peterson, D. K., Criswell, J. R. ir Crossland, M. D. (2006). *Privacy Policy Statements and Consumer Willingness to Provide Personal Information*. Journal of Electronic Commerce in Organizations, 4(1), 1–17. doi:10.4018/jeco.2006010101

Namara, M. ir Knijnenburg, B. P. (2021). *The Differential Effect of Privacy-Related Trust on Groupware Application Adoption and Use during the COVID-19 pandemic*. Proc. ACM Hum.-Comput. Interact. 5, CSCW2, Article 405 (October 2021), 34 pages. DOI:<https://doi.org/10.1145/3479549>

Nikkhah, H. R., Balapour, A. ir Sabherwal, R. (2018). *Mobile Applications Security: Role of Privacy*. Emergent Research Forum (ERF). Twenty-fourth Americas Conference on

Information Systems, New Orleans. Prieiga internetu: https://www.academia.edu/41830586/Mobile_Applications_Security_Role_of_Privacy (Žiūrėta 2020-07-22)

Papadopoulos, E. P., Diamantaris, M., Papadopoulos, P., Petsas, T., Ioannidis, S. ir Markatos, E. P. (2017 balandžio 3 – 4 d.). *The Long-Standing Privacy Debate*. Proceedings of the 26th International Conference on World Wide Web - WWW '17, Perth, Australia. doi:10.1145/3038912.3052691

Paspatis, I., Tsohou, A. ir Kokolakis, S. (2018). *AppAware: A Model for Privacy Policy Visualization for Mobile Applications*. MCIS 2018 Proceedings, 3. Prieiga internetu: <https://aisel.aisnet.org/mcis2018/3> (2020-07-22)

Punyatoya, P. (2018). *Effects of cognitive and affective trust on online customer behavior*. Marketing Intelligence & Planning. Preiga internetu: <https://doi.org/10.1108/MIP-02-2018-0058>

Rajivan, P. ir Camp, L. J. (2016). *Influence of Privacy Attitude and Privacy Cue Framing on Android App Choices*. Symposium on Usable Privacy and Security (SOUPS) 2016, June 22–24, Denver, Colorado. Prieiga internetu: <https://bit.ly/3q2C1Co> (Žiūrėta 2020-04-15)

Reuter, C., Häusser, K., Bien, M. ir Herbert, F. (2019). *Between Effort and Security*. *Proceedings of Mensch Und Computer 2019 on - MuC'19*. doi:10.1145/3340764.3340770

Ruchi, A. ir Kumar, M. S. (2018). *PRIVACY AND SECURITY CONCERN OF CUSTOMERS DOING ONLINE SHOPPING - AN ANALYTICAL STUDY*. International Journal of Advanced Research in Computer Science, 9(1), 122-136.

Setiawan, P. ir Widanta, A. A. B. P. (2021). *The effect of trust on travel agent online use: Application of the technology acceptance model*. International Journal of Data and Network Science, 5(3), 173-182. Doi: 10.5267/j.ijdns.2021.6.015

Shin, D. H. (2010). *The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption*. Interacting with Computers, 22(5), 428–438. doi:10.1016/j.intcom.2010.05.001

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H. ir Borgthorsson, H. (2014). *Leakiness and creepiness in app space*. *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems - CHI '14*. doi:10.1145/2556288.2557421

Siegfried, N., Koch, O. ir Benlian, A. (2015). *Drivers of App Installation Likelihood – A Conjoint Analysis of Quality Signals in Mobile Ecosystems*. Prieiga internetu: <https://bit.ly/3EhkkUU> (Žiūrėta 2021-12-15)

Sreejesh, S., Anusree, M. R. ir Mitra, A. (2016). *Effect of information content and form on customers' attitude and transaction intention in mobile banking*. International Journal of Bank Marketing, 34(7), 1092–1113. doi:10.1108/ijbm-07-2015-0107

„Statista“ (2020 sausio 29d.). *Annual number of app downloads from the Google Play Store worldwide from 2016 to 2019*. Prieiga internetu: <https://bit.ly/3ci8Nrs>. (Žiūrėta 2020 – 02 – 25)

„Statista“ (2019 lapkričio 22d.). *Forecast of the smartphone user penetration rate in Lithuania from 2015 to 2022*. Prieiga internetu: <https://bit.ly/2PDkorp>. (Žiūrėta 2020 – 02 – 25)

„Statista“ (2021 kovo 19d.). *Share of global smartphone shipments by operating system from 2014 to 2023*. Prieiga internetu: <https://bit.ly/3aFkiKj> (Žiūrėta 2021 – 04 – 25)

Steinke, G. (2002). *Data privacy approaches from US and EU perspectives*. Telematics and Informatics, 19(2), 193–200. doi:10.1016/s0736-5853(01)00013-2

Strahilevitz, L. J. ir Kugler, M. B. (2016). *Is Privacy Policy Language Irrelevant to Consumers?* The Journal of Legal Studies, 45(S2), S69–S95. doi:10.1086/689933

Tay, S. W., Teh, P. S. ir Payne, S. J. (2021). *Reasoning about privacy in mobile application install decisions: Risk perception and framing*. International Journal of Human-Computer Studies, 145, 102517. doi:10.1016/j.ijhcs.2020.102517

Tam, C., Santos, D. ir Oliveira, T. (2018). *Exploring the influential factors of continuance intention to use mobile Apps: Extending the expectation confirmation model*. Information Systems Frontiers. doi:10.1007/s10796-018-9864-5

Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S. ir Serna, J. (2018). *PrivacyGuide. Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics - IWSPA '18*. doi:10.1145/3180445.3180447

Tsai, J. Y., Egelman, S., Cranor, L. ir Acquisti, A. (2011). *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*. Information Systems Research, 22(2), 254–268. doi:10.1287/isre.1090.0260

Vasconcelos, L., Barcellos, R., Viterbo, J., Bernardini, F., Boscarioli, C. ir Nunes, E. (2019). *How Factors that Influence Engagement Impact Users' Evaluations in Mobile App Stores*. Lecture Notes in Computer Science, 571–584. doi:10.1007/978-3-030-21902-4_40

Wang, E. S. T. ir Lin, R. L. (2016). *Perceived quality factors of location-based apps on trust, perceived privacy risk, and continuous usage intention*. Behaviour & Information Technology, 1–9. doi:10.1080/0144929x.2016.1143033

Wang, H. Y., Liao, C. ir Yang, L. H. (2013). *What Affects Mobile Application Use? The Roles of Consumption Values*. International Journal of Marketing Studies, 5(2). doi:10.5539/ijms.v5n2p11

Wogalter, M. S. (2018). *Communication-Human Information Processing (C-HIP) Model in Forensic Warning Analysis*. Proceedings of the 20th Congress of the International Ergonomics Association (IEA 2018), 761–769. doi:10.1007/978-3-319-96080-7_92

Wogalter, M. S., Mayhorn, C. B., Black, A., Luna, P., Lund, O. ir Walker, S. (2017). *Warning design. Information design: Research and practice*, 331-348. <https://doi.org/10.4324/9781315585680>

Wood, D., Jr. (2019). *Revamping the Privacy Policy: A Study on Informed Consent and User Interactions. Thesis.* Prieiga internetu: <https://baylor-ir.tdl.org/bitstream/handle/2104/10571/Wood%20Thesis.pdf?sequence=1> (Žiūrėta 2021-12-14)

Wottrich, V. M., van Reijmersdal, E. A. ir Smit, E. G. (2018). *The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns.* *Decision Support Systems*, 106, 44–52. doi:10.1016/j.dss.2017.12.003

Wilkinson., D., Bahirat, P., Namara, M., Lyu, J., Alsubhi, A., Qiu, J., Wisniewski, P. ir Knijnenburg, B. P. (2020). *Privacy at a Glance: The User-Centric Design of Glanceable Data Exposure Visualizations.* *Proceedings on Privacy Enhancing Technologies*, 2, 416–435. Doi: <https://doi.org/10.2478/popets-2020-0034>

Wilson, S., Schaub, F., Dara, A. A., Liu, F., Cherivirala, S., Leon, P. G., Andersen, M. S., Zimmeck, S., Sathyendra, K. M., Russell, N. C., Norton, T. B., Hovy, E., Reidenberg, J. ir Sadeh, N. (2016). *The creation and analysis of a Website privacy policy corpus.* 54th Annual Meeting of the Association for Computational Linguistics, ACL 2016 - Long Papers; Vol. 3. Association for Computational Linguistics (ACL). <https://doi.org/10.18653/v1/p16-1126>

Wu, K.-W., Huang, S. Y., Yen, D. C. ir Popova, I. (2012). *The effect of online privacy policy on consumer privacy concern and trust.* *Computers in Human Behavior*, 28(3), 889–897. doi:10.1016/j.chb.2011.12.008

Zhang, B. ir Xu, H. (2016). *Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes.* *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing - CSCW '16.* doi:10.1145/2818048.2820073

Zhang, T., Lu, C. ir Kizildag, M. (2018). *Banking “on-the-go”: examining consumers’ adoption of mobile banking services.* *International Journal of Quality and Service Sciences.* doi:10.1108/ijqss-07-2017-0067

Zhao, J., Binns, R., Van Kleek, M. ir Shadbolt, N. (2016). *Privacy Languages. Proceedings of the 25th International Conference Companion on World Wide Web - WWW '16 Companion.* doi:10.1145/2872518.2890590

Zhong, N. ir Michahelles, F. (2013). *Google play is not a long tail market. Proceedings of the 28th Annual ACM Symposium on Applied Computing - SAC '13.* doi:10.1145/2480362.2480460

Zhou, T. (2017). *Understanding location-based services users’ privacy concern: an*

elaboration likelihood model. Perspective. Internet Research, 27(3). doi: 10.1108/IntR-04-2016-0088

Zimmer, J. C., Aarsal, R. E., Al-Marzouq, M. ir Grover, V. (2010). *Investigating online information disclosure: Effects of information relevance, trust and risk*. Information & Management, 47(2), 115–123. doi:10.1016/j.im.2009.12.003

2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB. Prieiga internetu: <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32018R1725> (Žiūrėta 2020-02-06)

PRIEDAI

1 priedas

Respondentų pasiskirstymas pagal lytį

		Frequency	Percent	Valid Percent	Cumulative Percent
Lytis	moteris	248	50,6	50,6	50,6
	vyras	242	49,4	49,4	100,0
	Total	490	100,0	100,0	

Respondentų pasiskirstymas pagal lytį skirtingose anketose

			ANKETA				Total
			A	B	C	D	
Lytis	moteris	Count	80	54	54	60	248
		Expected Count	69,8	57,7	54,7	65,8	248,0
		% within ANKETA	58,0%	47,4%	50,0%	46,2%	50,6%
	vyras	Count	58	60	54	70	242
		Expected Count	68,2	56,3	53,3	64,2	242,0
		% within ANKETA	42,0%	52,6%	50,0%	53,8%	49,4%
Total		Count	138	114	108	130	490
		Expected Count	138,0	114,0	108,0	130,0	490,0
		% within ANKETA	100,0%	100,0%	100,0%	100,0%	100,0%

2 priedas

Respondentų pasiskirstymas pagal amžių

Crosstab							
			ANKETA				Total
			A	B	C	D	
amzius	18	Count	0	0	4	0	4
		Expected Count	1,1	,9	,9	1,1	4,0
		% within ANKETA	0,0%	0,0%	3,7%	0,0%	0,8%
	19	Count	6	12	10	12	40
		Expected Count	11,3	9,3	8,8	10,6	40,0
		% within ANKETA	4,3%	10,5%	9,3%	9,2%	8,2%
	20	Count	14	8	2	6	30

		Expected Count	8,4	7,0	6,6	8,0	30,0
		% within ANKETA	10,1%	7,0%	1,9%	4,6%	6,1%
	21	Count	6	8	4	4	22
		Expected Count	6,2	5,1	4,8	5,8	22,0
		% within ANKETA	4,3%	7,0%	3,7%	3,1%	4,5%
	22	Count	12	6	6	20	44
		Expected Count	12,4	10,2	9,7	11,7	44,0
		% within ANKETA	8,7%	5,3%	5,6%	15,4%	9,0%
	23	Count	16	8	6	14	44
		Expected Count	12,4	10,2	9,7	11,7	44,0
		% within ANKETA	11,6%	7,0%	5,6%	10,8%	9,0%
	24	Count	14	6	10	8	38
		Expected Count	10,7	8,8	8,4	10,1	38,0
		% within ANKETA	10,1%	5,3%	9,3%	6,2%	7,8%
	25	Count	30	22	8	10	70
		Expected Count	19,7	16,3	15,4	18,6	70,0
		% within ANKETA	21,7%	19,3%	7,4%	7,7%	14,3%
	26	Count	8	2	8	14	32
		Expected Count	9,0	7,4	7,1	8,5	32,0
		% within ANKETA	5,8%	1,8%	7,4%	10,8%	6,5%
	27	Count	4	2	8	4	18
		Expected Count	5,1	4,2	4,0	4,8	18,0
		% within ANKETA	2,9%	1,8%	7,4%	3,1%	3,7%
	28	Count	4	2	6	2	14
		Expected Count	3,9	3,3	3,1	3,7	14,0
		% within ANKETA	2,9%	1,8%	5,6%	1,5%	2,9%
	29	Count	6	0	4	2	12
		Expected Count	3,4	2,8	2,6	3,2	12,0
		% within ANKETA	4,3%	0,0%	3,7%	1,5%	2,4%
	30	Count	2	6	6	6	20
		Expected Count	5,6	4,7	4,4	5,3	20,0
		% within ANKETA	1,4%	5,3%	5,6%	4,6%	4,1%
	31	Count	2	4	4	2	12
		Expected Count	3,4	2,8	2,6	3,2	12,0
		% within ANKETA	1,4%	3,5%	3,7%	1,5%	2,4%
	32	Count	4	2	2	4	12
		Expected Count	3,4	2,8	2,6	3,2	12,0
		% within ANKETA	2,9%	1,8%	1,9%	3,1%	2,4%
	33	Count	2	4	2	2	10
		Expected Count	2,8	2,3	2,2	2,7	10,0
		% within ANKETA	1,4%	3,5%	1,9%	1,5%	2,0%
	34	Count	2	4	0	0	6

		Expected Count	1,7	1,4	1,3	1,6	6,0
		% within ANKETA	1,4%	3,5%	0,0%	0,0%	1,2%
	36	Count	2	2	0	4	8
		Expected Count	2,3	1,9	1,8	2,1	8,0
		% within ANKETA	1,4%	1,8%	0,0%	3,1%	1,6%
	37	Count	0	2	6	0	8
		Expected Count	2,3	1,9	1,8	2,1	8,0
		% within ANKETA	0,0%	1,8%	5,6%	0,0%	1,6%
	38	Count	0	0	0	2	2
		Expected Count	,6	,5	,4	,5	2,0
		% within ANKETA	0,0%	0,0%	0,0%	1,5%	0,4%
	39	Count	0	0	0	6	6
		Expected Count	1,7	1,4	1,3	1,6	6,0
		% within ANKETA	0,0%	0,0%	0,0%	4,6%	1,2%
	40	Count	0	0	2	0	2
		Expected Count	,6	,5	,4	,5	2,0
		% within ANKETA	0,0%	0,0%	1,9%	0,0%	0,4%
	41	Count	0	0	0	2	2
		Expected Count	,6	,5	,4	,5	2,0
		% within ANKETA	0,0%	0,0%	0,0%	1,5%	0,4%
	42	Count	2	0	2	0	4
		Expected Count	1,1	,9	,9	1,1	4,0
		% within ANKETA	1,4%	0,0%	1,9%	0,0%	0,8%
	44	Count	0	4	0	0	4
		Expected Count	1,1	,9	,9	1,1	4,0
		% within ANKETA	0,0%	3,5%	0,0%	0,0%	0,8%
	45	Count	0	0	2	0	2
		Expected Count	,6	,5	,4	,5	2,0
		% within ANKETA	0,0%	0,0%	1,9%	0,0%	0,4%
	46	Count	0	2	0	2	4
		Expected Count	1,1	,9	,9	1,1	4,0
		% within ANKETA	0,0%	1,8%	0,0%	1,5%	0,8%
	47	Count	2	2	2	0	6
		Expected Count	1,7	1,4	1,3	1,6	6,0
		% within ANKETA	1,4%	1,8%	1,9%	0,0%	1,2%
	49	Count	0	2	0	0	2
		Expected Count	,6	,5	,4	,5	2,0
		% within ANKETA	0,0%	1,8%	0,0%	0,0%	0,4%
	50	Count	0	0	2	0	2
		Expected Count	,6	,5	,4	,5	2,0
		% within ANKETA	0,0%	0,0%	1,9%	0,0%	0,4%
	51	Count	0	0	2	0	2

		Expected Count	,6	,5	,4	,5	2,0
		% within ANKETA	0,0%	0,0%	1,9%	0,0%	0,4%
	53	Count	0	0	0	2	2
		Expected Count	,6	,5	,4	,5	2,0
		% within ANKETA	0,0%	0,0%	0,0%	1,5%	0,4%
	54	Count	0	0	0	2	2
		Expected Count	,6	,5	,4	,5	2,0
		% within ANKETA	0,0%	0,0%	0,0%	1,5%	0,4%
	56	Count	0	2	0	0	2
		Expected Count	,6	,5	,4	,5	2,0
		% within ANKETA	0,0%	1,8%	0,0%	0,0%	0,4%
	59	Count	0	2	0	0	2
		Expected Count	,6	,5	,4	,5	2,0
		% within ANKETA	0,0%	1,8%	0,0%	0,0%	0,4%
Total	Count		138	114	108	130	490
	Expected Count		138,0	114,0	108,0	130,0	490,0
	% within ANKETA		100,0%	100,0%	100,0%	100,0%	100,0%

3 priedas

Skalių patikimumas

Suvokiamą riziką matuojančios skalės Chronbach Alpha:

Reliability Statistics	
Cronbach's Alpha	N of Items
,943	6

Item-Total Statistics				
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
SUVOK RIZ 1	18,53	60,826	,785	,937
SUVOK RIZ 2	18,30	58,961	,831	,932
SUVOK RIZ 3	18,51	59,183	,823	,933
SUVOK RIZ 4	18,59	58,975	,838	,931
SUVOK RIZ 5	18,43	58,021	,858	,928
SUVOK RIZ 6	18,70	58,482	,827	,932

Požiūrio į aplikaciją matuojančios skalės Chronbach Alpha:

Reliability Statistics	
Cronbach's Alpha	N of Items
,934	4

Item-Total Statistics				
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
POZIUR 1	14,23	20,601	,821	,920
POZIUR 2	14,11	20,273	,861	,908
POZIUR 3	14,13	20,167	,867	,906
POZIUR 4	14,24	19,617	,828	,919

Suvokiamo pasitikėjimo matuojančios skalės Chronbach Alpha:

Reliability Statistics	
Cronbach's Alpha	N of Items
,922	5

Item-Total Statistics				
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
PASITIK 1	16,93	30,376	,771	,909
PASITIK 2	16,93	30,807	,780	,908
PASITIK 3	16,84	29,583	,804	,903
PASITIK 4	16,78	28,603	,821	,899
PASITIK 5	16,87	29,251	,811	,901

Ketinimo įsidiesti aplikaciją matuojančios skalės Chronbach Alpha:

Reliability Statistics	
Cronbach's Alpha	N of Items
,943	5

Item-Total Statistics				
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
KETINIM 1	17,15	40,601	,844	,931
KETINIM 2	17,12	40,090	,850	,929
KETINIM 3	17,14	38,582	,862	,927
KETINIM 4	16,79	38,957	,849	,929
KETINIM 5	17,28	38,968	,827	,934

Privatumo politikos pateikimo formatus matuojančios skalės Chronbach Alpha:

Reliability Statistics	
Cronbach's Alpha	N of Items
,878	3

Item-Total Statistics				
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
VIZULK 1	9,64	10,149	,688	,893
VIZULK 2	9,79	8,582	,815	,781
VIZULK 3	9,64	8,832	,796	,798

Westin indeksą matuojančios skalės Chronbach Alpha:

Reliability Statistics	
Cronbach's Alpha	N of Items
,787	2

Item-Total Statistics				
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
WESTIN2	4,40	2,007	,648	.
WESTIN3	4,23	2,019	,648	.

4 priedas

Faktorinė analizė - Varimax pasuktos matricos principas

Communalities		
	Initial	Extraction
Mano požiūris į šią aplikaciją yra teigiamas	1,000	,627
Manau, kad ši aplikacija patenkins mano lūkesčius	1,000	,706
Mano požiūris į šią aplikaciją yra priimtinas	1,000	,731
Mano požiūris į šią aplikaciją yra malonus	1,000	,667
Daugelis įmonių tinkamai ir konfidencialiai tvarko asmeninę informaciją, kurią renka apie vartotojus	1,000	,807
Galiojantys įstatymai ir organizacinė praktika užtikrina pagrįstą vartotojų privatumo apsaugos lygį šiandien.	1,000	,809
Manau, kad ši aplikacija perduos asmeninę informaciją be mano leidimo	1,000	,725
Manau, kad ši aplikacija gali pakenkti mano privatumui	1,000	,783
Manau, kad asmeninės informacijos pateikimas šiai aplikacijai galėtų sukelti daug neaiškumų	1,000	,768
Manau, kad susidurčiau su daugeliu problemų, pateikęs (-usi) savo asmeninę informaciją šiai aplikacijai	1,000	,795
Pateikti asmeninę informaciją šiai programai būtų rizikinga	1,000	,813
Manau, kad asmeninės informacijos pateikimas šiai aplikacijai sukeltų daug galimų nuostolių	1,000	,779
Šios aplikacijos kūrėjai būtų patikimi tvarkydami mano informaciją	1,000	,629
Šios aplikacijos kūrėjai pasakytų tiesą ir vykdytų pažadus susijusius su mano pateikta informacija	1,000	,605
Tikiu, kad šios aplikacijos kūrėjai tvarkydami informaciją, nepamirštų mano interesų	1,000	,702
Šios aplikacijos kūrėjai yra nuspėjami ir nuoseklūs informacijos naudojimo atžvilgiu	1,000	,689
Šios aplikacijos kūrėjai visada sąžiningai elgtųsi su klientais, kai reiktų naudoti mano pateiktą informaciją	1,000	,669
Manau, kad pateiktas privatumo pranešimas padėjo man suprasti galimas grėsmes, su kuriomis galiu susidurti	1,000	,717
Manau, kad pateiktas privatumo pranešimas buvo lengvai skaitomas	1,000	,860
Manau, kad pateiktas privatumo pranešimas buvo lengvai suprantamas	1,000	,832
Jei turėsiu galimybę, naudosiuosi šia aplikacija	1,000	,734
Manau, kad svarstyčiau įsidięgti šią aplikaciją	1,000	,721
Aš ketinčiau įsidięgti šią aplikaciją	1,000	,775
Tikėtina, kad naudočiau šią aplikaciją, kai ji man bus reikalinga	1,000	,725
Manau, kad rekomenduočiau šią aplikaciją savo draugams.	1,000	,717
Extraction Method: Principal Component Analysis.		

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,956
Bartlett's Test of Sphericity	Approx. Chi-Square	11114,598
	df	300
	Sig.	,000

Total Variance Explained

Component	Total	Initial Eigenvalues		Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
		% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	13,314	53,255	53,255	13,314	53,255	53,255	8,641	34,564	34,564
2	2,091	8,364	61,619	2,091	8,364	61,619	5,285	21,141	55,705
3	1,682	6,728	68,347	1,682	6,728	68,347	2,759	11,035	66,741
4	1,300	5,200	73,547	1,300	5,200	73,547	1,701	6,806	73,547
5	,871	3,483	77,030						
6	,837	3,348	80,378						
7	,468	1,873	82,251						
8	,395	1,579	83,830						
9	,391	1,565	85,395						
10	,341	1,365	86,760						
11	,328	1,313	88,073						
12	,312	1,249	89,323						
13	,289	1,154	90,477						
14	,267	1,068	91,545						
15	,259	1,037	92,581						
16	,242	,968	93,549						
17	,225	,901	94,450						
18	,215	,860	95,310						
19	,205	,819	96,129						
20	,197	,788	96,918						
21	,176	,704	97,622						
22	,169	,676	98,298						
23	,162	,648	98,946						
24	,149	,597	99,543						
25	,114	,457	100,000						

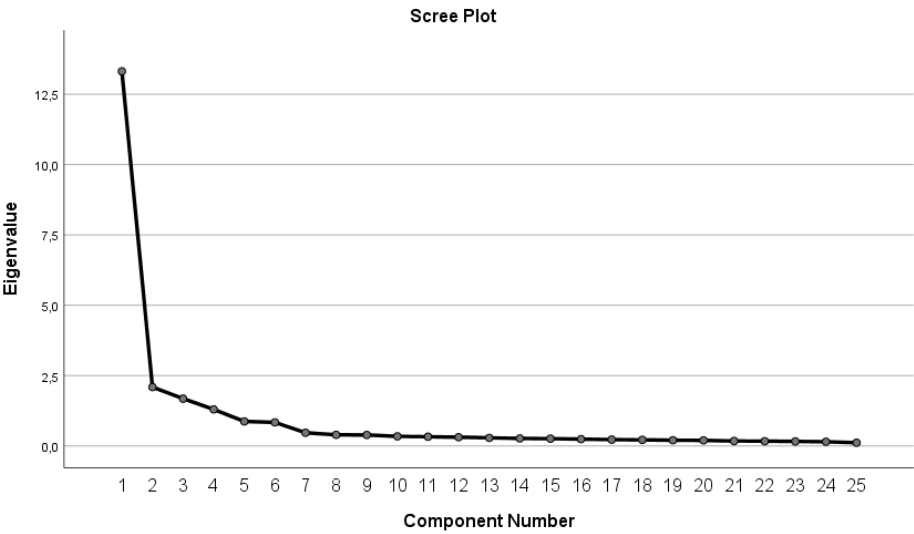
Extraction Method: Principal Component Analysis.

Rotated Component Matrix ^a				
	Component			
	1	2	3	4
Aš ketinčiau įsdiegti šią aplikaciją	,810	,219	,266	
Manau, kad svarstyčiau įsdiegti šią aplikaciją	,786	,249		
Tikėtina, kad naudočiau šią aplikaciją, kai ji man bus reikalinga	,778	,280		
Jei turėsiu galimybę, naudosisiu šia aplikacija	,766	,319	,207	
Manau, kad ši aplikacija patenkins mano lūkesčius	,751	,360		
Manau, kad rekomenduočiau šią aplikaciją savo draugams.	,741	,218	,332	
Tikiu, kad šios aplikacijos kūrėjai tvarkydami informaciją, nepamirštų mano interesų	,739	,347		
Mano požiūris į šią aplikaciją yra priimtinas	,738	,413		
Šios aplikacijos kūrėjai visada sąžiningai elgtųsi su klientais, kai reiktų naudoti mano pateiktą informaciją	,732	,300	,201	
Mano požiūris į šią aplikaciją yra malonus	,716	,299	,257	
Šios aplikacijos kūrėjai yra nuspėjami ir nuoseklūs informacijos naudojimo atžvilgiu	,710	,363		
Šios aplikacijos kūrėjai pasakytų tiesą ir vykdytų pažadus susijusius su mano pateikta informacija	,695	,314		
Mano požiūris į šią aplikaciją yra teigiamas	,670	,391		
Šios aplikacijos kūrėjai būtų patikimi tvarkydami mano informaciją	,662	,413		
Manau, kad susidurčiau su daugeliu problemų, pateikęs (-usi) savo asmeninę informaciją šiai aplikacijai	-,363	-,812		
Manau, kad asmeninės informacijos pateikimas šiai aplikacijai sukeltų daug galimų nuostolių	-,350	-,803		
Manau, kad asmeninės informacijos pateikimas šiai aplikacijai galėtų sukelti daug neaiškumų	-,346	-,793		
Pateikti asmeninę informaciją šiai programai būtų rizikinga	-,420	-,788		
Manau, kad ši aplikacija gali pakenkti mano privatumui	-,367	-,786		
Manau, kad ši aplikacija perduos asmeninę informaciją be mano leidimo	-,378	-,762		
Manau, kad pateiktas privatumo pranešimas buvo lengvai skaitomas	,250		,889	
Manau, kad pateiktas privatumo pranešimas buvo lengvai suprantamas	,336		,844	
Manau, kad pateiktas privatumo pranešimas padėjo man suprasti galimas grėsmes, su kuriomis galiu susidurti	,206		,803	
Galiojantys įstatymai ir organizacinė praktika užtikrina pagrįstą vartotojų privatumo apsaugos lygį šiandien.				,898
Daugelis įmonių tinkamai ir konfidencialiai tvarko asmeninę informaciją, kurią renka apie vartotojus				,897
Extraction Method: Principal Component Analysis.				
Rotation Method: Varimax with Kaiser Normalization.				
a. Rotation converged in 5 iterations.				

Component Transformation Matrix

Component	1	2	3	4
1	,781	,553	,289	,027
2	,157	-,621	,749	,169
3	-,026	,071	-,157	,985
4	,604	-,551	-,575	-,036

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.



Correlation Matrix^a

		POZIUR 1	POZIUR 2	POZIUR 3	POZIUR 4	WESTIN2	WESTIN3	SUVOK RIZ 1	SUVOK RIZ 2	SUVOK RIZ 3	SUVOK RIZ 4	SUVOK RIZ 5	SUVOK RIZ 6	PASITIK 1	PASITIK 2	PASITIK 3	PASITIK 4	PASITIK 5	VIZULK 1	VIZULK 2	VIZULK 3	KETINIM 1	KETINIM 2	KETINIM 3	KETINIM 4	KETINIM 5
Correlation	POZIUR 1	1,000	,779	,760	,751	,043	,062	-,545	-,577	-,541	-,527	-,610	-,537	,591	,532	,621	,612	,547	,355	,349	,362	,593	,576	,629	,583	,574
	POZIUR 2	,779	1,000	,836	,761	,005	,044	-,535	-,575	-,527	-,601	-,588	-,546	,602	,579	,666	,625	,614	,320	,338	,373	,670	,636	,668	,617	,610
	POZIUR 3	,760	,836	1,000	,793	,006	,053	-,571	-,608	-,579	-,614	-,637	-,587	,623	,614	,636	,669	,620	,352	,337	,381	,669	,656	,660	,669	,615
	POZIUR 4	,751	,761	,793	1,000	,044	,029	-,488	-,543	-,499	-,505	-,576	-,519	,566	,556	,625	,600	,606	,377	,430	,490	,603	,606	,663	,621	,665
	WESTIN2	,043	,005	,006	,044	1,000	,648	,008	-,015	-,048	,019	,017	,032	,005	,064	,089	,100	,023	,038	,055	,061	-,023	-,028	,031	-,012	-,014
	WESTIN3	,062	,044	,053	,029	,648	1,000	-,044	-,032	-,048	-,034	-,008	-,018	,064	,096	,123	,134	,068	,045	,025	,062	,044	,015	,093	,028	-,031
	SUVOK RIZ 1	-,545	-,535	-,571	-,488	,008	-,044	1,000	,752	,682	,689	,705	,682	-,579	-,495	-,549	-,529	-,515	-,228	-,189	-,226	-,561	-,503	-,505	-,516	-,457
	SUVOK RIZ 2	-,577	-,575	-,608	-,543	-,015	-,032	,752	1,000	,757	,727	,747	,702	-,565	-,509	-,561	-,566	-,527	-,324	-,303	-,326	-,568	-,520	-,551	-,537	-,532
	SUVOK RIZ 3	-,541	-,527	-,579	-,499	-,048	-,048	,682	,757	1,000	,756	,751	,706	-,534	-,488	-,520	-,570	-,504	-,302	-,271	-,270	-,575	-,527	-,527	-,558	-,518
	SUVOK RIZ 4	-,527	-,601	-,614	-,505	,019	-,034	,689	,727	,756	1,000	,767	,766	-,562	-,492	-,555	-,567	-,511	-,250	-,228	-,242	-,553	-,527	-,480	-,547	-,479
	SUVOK RIZ 5	-,610	-,588	-,637	-,576	,017	-,008	,705	,747	,751	,767	1,000	,807	-,587	-,560	-,601	-,573	-,579	-,283	-,283	-,310	-,600	-,558	-,560	-,556	-,543
	SUVOK RIZ 6	-,537	-,546	-,587	-,519	,032	-,018	,682	,702	,706	,766	,807	1,000	-,588	-,497	-,552	-,525	-,530	-,283	-,251	-,276	-,553	-,510	-,490	-,551	-,480
	PASITIK 1	,591	,602	,623	,566	,005	,064	-,579	-,565	-,534	-,562	-,587	-,588	1,000	,673	,670	,706	,685	,355	,311	,380	,618	,602	,613	,616	,549
	PASITIK 2	,532	,579	,614	,556	,064	,096	-,495	-,509	-,488	-,492	-,560	-,497	,673	1,000	,684	,707	,696	,330	,284	,355	,599	,565	,588	,568	,543
	PASITIK 3	,621	,666	,636	,625	,089	,123	-,549	-,561	-,520	-,555	-,601	-,552	,670	,684	1,000	,735	,738	,332	,343	,408	,651	,627	,660	,650	,607
	PASITIK 4	,612	,625	,669	,600	,100	,134	-,529	-,566	-,570	-,567	-,573	-,525	,706	,707	,735	1,000	,729	,382	,369	,411	,636	,621	,644	,630	,566
	PASITIK 5	,547	,614	,620	,606	,023	,068	-,515	-,527	-,504	-,511	-,579	-,530	,685	,696	,738	,729	1,000	,347	,404	,453	,659	,602	,672	,638	,623
	VIZULK 1	,355	,320	,352	,377	,038	,045	-,228	-,324	-,302	-,250	-,283	-,283	,355	,330	,332	,382	,347	1,000	,666	,642	,389	,354	,386	,363	,384
	VIZULK 2	,349	,338	,337	,430	,055	,025	-,189	-,303	-,271	-,228	-,283	-,251	,311	,284	,343	,369	,404	,666	1,000	,806	,390	,370	,453	,362	,504
	VIZULK 3	,362	,373	,381	,490	,061	,062	-,226	-,326	-,270	-,242	-,310	-,276	,380	,355	,408	,411	,453	,642	,806	1,000	,431	,424	,499	,447	,510
	KETINIM 1	,593	,670	,669	,603	-,023	,044	-,561	-,568	-,575	-,553	-,600	-,553	,618	,599	,651	,636	,659	,389	,390	,431	1,000	,786	,769	,779	,740
	KETINIM 2	,576	,636	,656	,606	-,028	,015	-,503	-,520	-,527	-,527	-,558	-,510	,602	,565	,627	,621	,602	,354	,370	,424	,786	1,000	,786	,773	,748
	KETINIM 3	,629	,668	,660	,663	,031	,093	-,505	-,551	-,527	-,480	-,560	-,490	,613	,588	,660	,644	,672	,386	,453	,499	,786	,786	1,000	,786	,784
	KETINIM 4	,583	,617	,669	,621	-,012	,028	-,516	-,537	-,558	-,547	-,556	-,551	,616	,568	,650	,630	,638	,363	,362	,447	,779	,773	,786	1,000	,750
	KETINIM 5	,574	,610	,615	,665	-,014	-,031	-,457	-,532	-,518	-,479	-,543	-,480	,549	,543	,600	,567	,623	,384	,504	,510	,740	,748	,784	,750	1,000
Sig. (1-tailed)	POZIUR 1		,000	,000	,000	,173	,086	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	POZIUR 2	,000		,000	,000	,460	,164	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	POZIUR 3	,000	,000		,000	,448	,122	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	POZIUR 4	,000	,000	,000		,164	,261	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	WESTIN2	,173	,460	,448	,164		,000	,426	,367	,145	,337	,351	,242	,458	,079	,024	,013	,306	,202	,111	,090	,303	,267	,246	,395	,375
	WESTIN3	,086	,164	,122	,261	,000		,164	,237	,144	,227	,430	,345	,079	,017	,003	,001	,066	,161	,288	,086	,167	,366	,020	,271	,243
	SUVOK RIZ 1	,000	,000	,000	,000	,426	,164		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	SUVOK RIZ 2	,000	,000	,000	,000	,367	,237	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	SUVOK RIZ 3	,000	,000	,000	,000	,145	,144	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	SUVOK RIZ 4	,000	,000	,000	,000	,337	,227	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	SUVOK RIZ 5	,000	,000	,000	,000	,351	,430	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	SUVOK RIZ 6	,000	,000	,000	,000	,242	,345	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	PASITIK 1	,000	,000	,000	,000	,458	,079	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	PASITIK 2	,000	,000	,000	,000	,079	,017	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	PASITIK 3	,000	,000	,000	,000	,024	,003	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	PASITIK 4	,000	,000	,000	,000	,013	,001	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000
	PASITIK 5	,000	,000	,000	,000	,306	,066	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000
	VIZULK 1	,000	,000	,000	,000	,202	,161	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000
	VIZULK 2	,000	,000	,000	,000	,111	,288	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000
	VIZULK 3	,000	,000	,000	,000	,090	,086	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000
	KETINIM 1	,000	,000	,000	,000	,303	,167	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000
	KETINIM 2	,000	,000	,000	,000	,267	,366	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000
	KETINIM 3	,000	,000	,000	,000	,246	,020	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000
	KETINIM 4	,000	,000	,000	,000	,395	,271	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000
	KETINIM 5	,000	,000	,000	,000	,375	,243	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	

a. Determinant = 8,714E-11

5 priedas

Tiesinės regresijos rezultatai

H1:

Descriptive Statistics				Correlations			
	Mean	Std. Deviation	N		Suv_riz	POLITIKA	
Suv_riz	3,7020	1,52849	490	Pearson Correlation	Suv_riz	1,000	,200
POLITIKA	1,50	,501	490		POLITIKA	,200	1,000
				Sig. (1-tailed)	Suv_riz		,000
					POLITIKA	,000	
				N	Suv_riz	490	490
					POLITIKA	490	490

Model Summary ^b				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,200 ^a	,040	,038	1,49927

a. Predictors: (Constant), POLITIKA

b. Dependent Variable: Suv_riz

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	45,511	1	45,511	20,247	,000 ^b
	Residual	1096,931	488	2,248		
	Total	1142,442	489			

a. Dependent Variable: Suv_riz

b. Predictors: (Constant), POLITIKA

Coefficients ^a								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	2,788	,214		13,016	,000		
	POLITIKA	,610	,135	,200	4,500	,000	1,000	1,000

a. Dependent Variable: Suv_riz

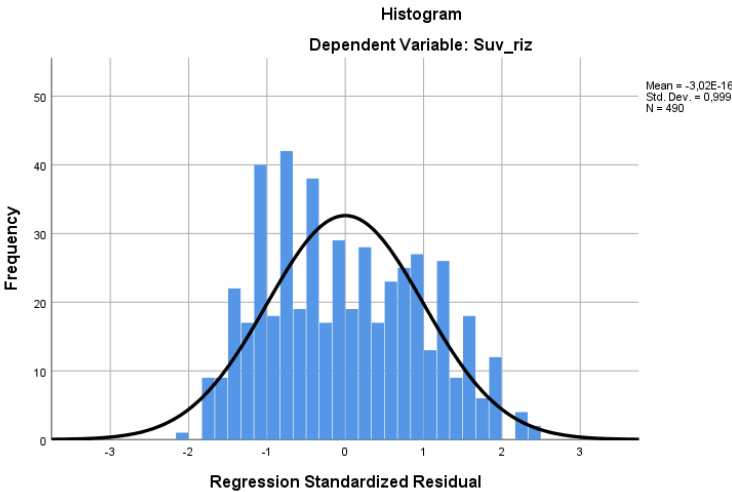
Collinearity Diagnostics ^a					
Model	Dimension	Eigenvalue	Condition Index	Variance Proportions	
				(Constant)	POLITIKA
1	1	1,949	1,000	,03	,03
	2	,051	6,162	,97	,97

a. Dependent Variable: Suv_riz

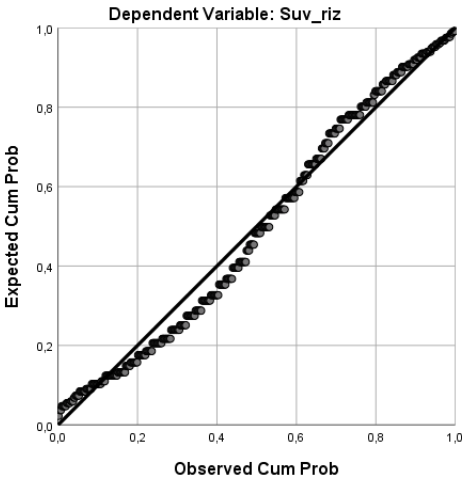
Residuals Statistics^a

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	3,3973	4,0068	3,7020	,30507	490
Std. Predicted Value	-,999	,999	,000	1,000	490
Standard Error of Predicted Value	,096	,096	,096	,000	490
Adjusted Predicted Value	3,3825	4,0191	3,7020	,30514	490
Residual	-3,00680	3,60272	,00000	1,49774	490
Std. Residual	-2,006	2,403	,000	,999	490
Stud. Residual	-2,010	2,408	,000	1,001	490
Deleted Residual	-3,01913	3,61749	,00000	1,50387	490
Stud. Deleted Residual	-2,016	2,420	,000	1,002	490
Mahal. Distance	,998	,998	,998	,000	490
Cook's Distance	,000	,012	,002	,002	490
Centered Leverage Value	,002	,002	,002	,000	490

a. Dependent Variable: Suv_riz



Normal P-P Plot of Regression Standardized Residual



6 priedas

H2 regresija:

Descriptive Statistics			
	Mean	Std. Deviation	N
Pasitik	4,2176	1,34985	490
POLITIKA	1,50	,501	490

Correlations

		Pasitik	POLITIKA
Pearson Correlation	Pasitik	1,000	-,229
	POLITIKA	-,229	1,000
Sig. (1-tailed)	Pasitik	.	,000
	POLITIKA	,000	.
N	Pasitik	490	490
	POLITIKA	490	490

Model Summary^b

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,229 ^a	,053	,051	1,31529

a. Predictors: (Constant), POLITIKA

b. Dependent Variable: Pasitik

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	46,780	1	46,780	27,041	,000 ^b
	Residual	844,230	488	1,730		
	Total	891,009	489			

a. Dependent Variable: Pasitik

b. Predictors: (Constant), POLITIKA

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	5,144	,188		27,379	,000		
	POLITIKA	-,618	,119	-,229	-5,200	,000	1,000	1,000

a. Dependent Variable: Pasitik

Collinearity Diagnostics^a

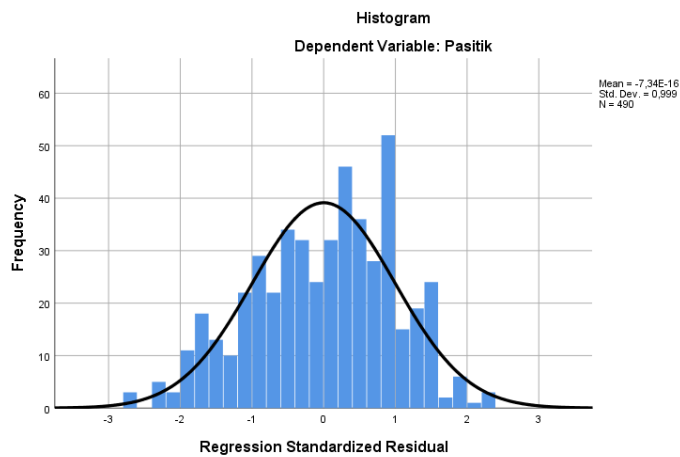
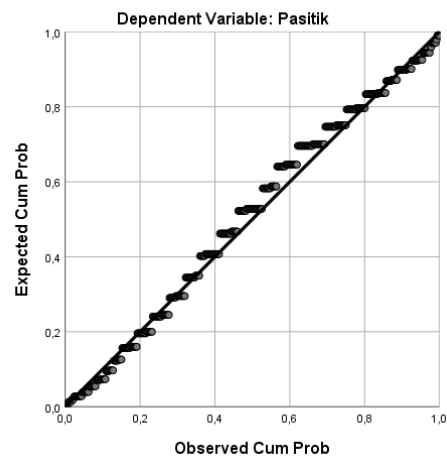
Model	Dimension	Eigenvalue	Condition Index	Variance Proportions	
				(Constant)	POLITIKA
1	1	1,949	1,000	,03	,03
	2	,051	6,162	,97	,97

a. Dependent Variable: Pasitik

Residuals Statistics^a

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	3,9086	4,5265	4,2176	,30930	490
Std. Predicted Value	-,999	,999	,000	1,000	490
Standard Error of Predicted Value	,084	,084	,084	,000	490
Adjusted Predicted Value	3,8959	4,5410	4,2176	,30934	490
Residual	-3,52653	3,09143	,00000	1,31394	490
Std. Residual	-2,681	2,350	,000	,999	490
Stud. Residual	-2,687	2,355	,000	1,001	490
Deleted Residual	-3,54098	3,10410	,00000	1,31933	490
Stud. Deleted Residual	-2,704	2,366	,000	1,003	490
Mahal. Distance	,998	,998	,998	,000	490
Cook's Distance	,000	,015	,002	,003	490
Centered Leverage Value	,002	,002	,002	,000	490

a. Dependent Variable: Pasitik

Normal P-P Plot of Regression Standardized Residual

7 priedas

H4 regresija

Correlations

				Poz_apl	Suv_riz
Descriptive Statistics					
	Mean	Std. Deviation	N		
Poz_apl	4,7265	1,48052	490		
Suv_riz	3,7020	1,52849	490		

		Poz_apl	Suv_riz
Pearson Correlation	Poz_apl	1,000	-,694
	Suv_riz	-,694	1,000
Sig. (1-tailed)	Poz_apl	.	,000
	Suv_riz	,000	.
N	Poz_apl	490	490
	Suv_riz	490	490

Model Summary^b

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,694 ^a	,482	,480	1,06714

a. Predictors: (Constant), Suv_riz

b. Dependent Variable: Poz_apl

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	516,129	1	516,129	453,228	,000 ^b
	Residual	555,727	488	1,139		
	Total	1071,855	489			

a. Dependent Variable: Poz_apl

b. Predictors: (Constant), Suv_riz

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	7,215	,126		57,065	,000		
	Suv_riz	-,672	,032	-,694	-21,289	,000	1,000	1,000

a. Dependent Variable: Poz_apl

Collinearity Diagnostics^a

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions	
				(Constant)	Suv_riz
1	1	1,924	1,000	,04	,04
	2	,076	5,047	,96	,96

a. Dependent Variable: Poz_apl

Casewise Diagnostics^a

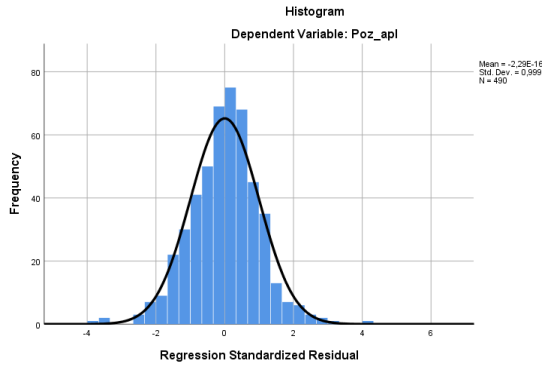
Case Number	Std. Residual	Poz_apl	Predicted Value	Residual
21	4,208	7,00	2,5098	4,49017
26	-3,578	2,50	6,3186	-3,81864
41	-3,837	2,00	6,0946	-4,09459
91	-3,393	2,25	5,8705	-3,62055
138	3,053	7,00	3,7421	3,25791

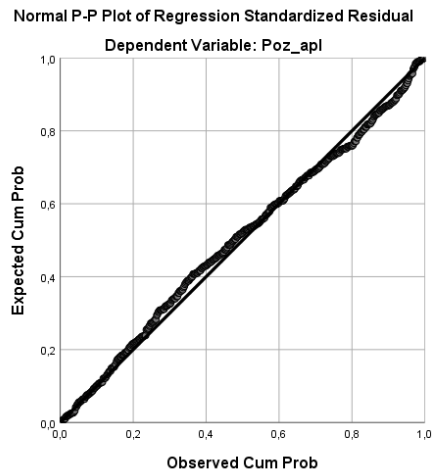
a. Dependent Variable: Poz_apl

Residuals Statistics^a

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	2,5098	6,5427	4,7265	1,02736	490
Std. Predicted Value	-2,158	1,768	,000	1,000	490
Standard Error of Predicted Value	,048	,115	,066	,016	490
Adjusted Predicted Value	2,4573	6,5452	4,7266	1,02740	490
Residual	-4,09459	4,49017	,00000	1,06605	490
Std. Residual	-3,837	4,208	,000	,999	490
Stud. Residual	-3,848	4,232	,000	1,001	490
Deleted Residual	-4,11793	4,54269	-,00004	1,07107	490
Stud. Deleted Residual	-3,904	4,308	,000	1,005	490
Mahal. Distance	,001	4,655	,998	,999	490
Cook's Distance	,000	,105	,002	,007	490
Centered Leverage Value	,000	,010	,002	,002	490

a. Dependent Variable: Poz_apl





8 priedas

H5 regresija

Descriptive Statistics				Correlations			
	Mean	Std. Deviation	N		Poz_apl	Pasitik	
Poz_apl	4,7265	1,48052	490	Pearson Correlation	Poz_apl	1,000	,759
Pasitik	4,2176	1,34985	490		Pasitik	,759	1,000
				Sig. (1-tailed)	Poz_apl	.	,000
					Pasitik	,000	.
				N	Poz_apl	490	490
					Pasitik	490	490

Model Summary ^b				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,759 ^a	,576	,575	,96509

a. Predictors: (Constant), Pasitik

b. Dependent Variable: Poz_apl

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	617,331	1	617,331	662,798	,000 ^b
	Residual	454,524	488	,931		
	Total	1071,855	489			

a. Dependent Variable: Poz_apl

b. Predictors: (Constant), Pasitik

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	1,216	,143		8,494	,000		
	Pasitik	,832	,032	,759	25,745	,000	1,000	1,000

a. Dependent Variable: Poz_apl

Collinearity Diagnostics^a

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions	
				(Constant)	Pasitik
1	1	1,952	1,000	,02	,02
	2	,048	6,411	,98	,98

a. Dependent Variable: Poz_apl

Casewise Diagnostics^a

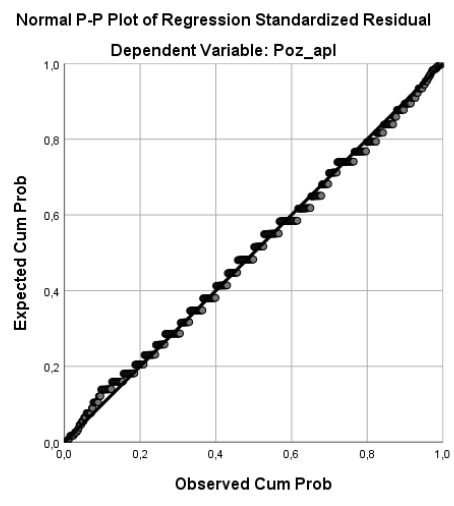
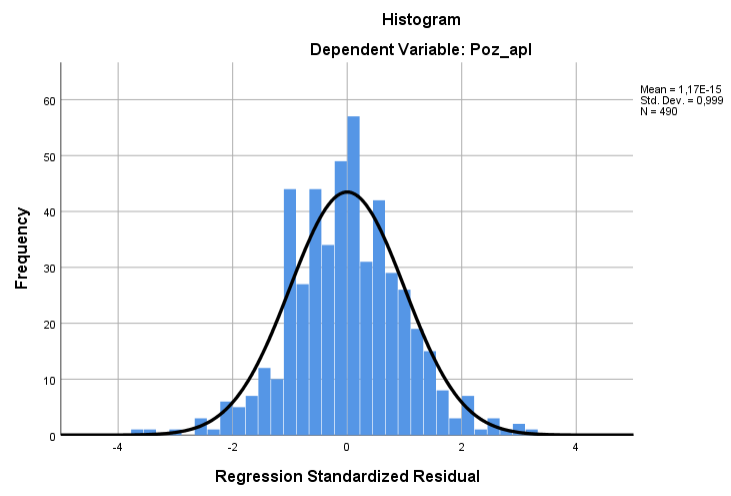
Case Number	Std. Residual	Poz_apl	Predicted Value	Residual
1	-3,672	2,50	6,0437	-3,54372
90	3,061	7,00	4,0460	2,95398
206	-3,415	1,25	4,5454	-3,29545
368	3,317	5,25	2,0483	3,20167

a. Dependent Variable: Poz_apl

Residuals Statistics^a

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	2,0483	7,0426	4,7265	1,12358	490
Std. Predicted Value	-2,384	2,061	,000	1,000	490
Standard Error of Predicted Value	,044	,113	,059	,016	490
Adjusted Predicted Value	2,0040	7,0620	4,7266	1,12384	490
Residual	-3,54372	3,20167	,00000	,96410	490
Std. Residual	-3,672	3,317	,000	,999	490
Stud. Residual	-3,681	3,340	,000	1,001	490
Deleted Residual	-3,56099	3,24601	-,00011	,96823	490
Stud. Deleted Residual	-3,729	3,376	,000	1,004	490
Mahal. Distance	,000	5,682	,998	1,202	490
Cook's Distance	,000	,077	,002	,005	490
Centered Leverage Value	,000	,012	,002	,002	490

a. Dependent Variable: Poz_apl



9 priedas

Požiūrio į aplikaciją bei ketinimo ją įsidięgti moderacija amžiaus atžvilgiu.

Run MATRIX procedure:

```
***** PROCESS Procedure for SPSS Version 4.0 *****  
  
Written by Andrew F. Hayes, Ph.D.      www.afhayes.com  
Documentation available in Hayes (2022). www.guilford.com/p/hayes3  
  
*****  
Model   : 1  
Y       : ketinim  
X       : Poz_apl  
W       : D2
```

Sample
Size: 490

OUTCOME VARIABLE:
ketinim

Model Summary

R	R-sq	MSE	F	df1	df2	p
,7629	,5820	1,0223	225,5360	3,0000	486,0000	,0000

Model

	coeff	se	t	p	LLCI	ULCI
constant	4,2742	,0457	93,4647	,0000	4,1844	4,3641
Poz_apl	,8015	,0309	25,9092	,0000	,7407	,8622
D2	,0054	,0061	,8872	,3754	-,0066	,0174
Int_1	,0001	,0042	,0259	,9793	-,0081	,0084

Product terms key:

Int_1 : Poz_apl x D2

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	,0000	,0007	1,0000	486,0000	,9793

Focal predict: Poz_apl (X)
Mod var: D2 (W)

Data for visualizing the conditional effect of the focal predictor:
Paste text below into a SPSS syntax window and execute to produce plot.

DATA LIST FREE/

Poz_apl D2 ketinim .
BEGIN DATA.

-1,4765	-5,9061	3,0598
,2735	-5,9061	4,4612
1,5235	-5,9061	5,4622
-1,4765	-1,9061	3,0808
,2735	-1,9061	4,4830
1,5235	-1,9061	5,4846
-1,4765	5,5339	3,1199
,2735	5,5339	4,5235
1,5235	5,5339	5,5261

END DATA.

GRAPH/SCATTERPLOT=

Poz_apl WITH ketinim BY D2 .

***** ANALYSIS NOTES AND ERRORS *****

Level of confidence for all confidence intervals in output:
95,0000

NOTE: The following variables were mean centered prior to analysis:
D2 Poz_apl

----- END MATRIX -----

10 priedas

Požiūrio į aplikaciją bei ketinimo ją įsdiegti moderacija lyties atžvilgiu.

Run MATRIX procedure:

***** PROCESS Procedure for SPSS Version 4.0 *****

Written by Andrew F. Hayes, Ph.D. www.afhayes.com
Documentation available in Hayes (2022). www.guilford.com/p/hayes3

Model : 1
Y : ketinim
X : Poz_apl
W : D1

Sample
Size: 490

OUTCOME VARIABLE:

ketinim

Model Summary

R	R-sq	MSE	F	df1	df2	p
,7628	,5818	1,0227	225,3874	3,0000	486,0000	,0000

Model

	coeff	se	t	p	LLCI	ULCI
constant	4,2664	,0642	66,4285	,0000	4,1402	4,3926
Poz_apl	,7804	,0423	18,4342	,0000	,6972	,8636
D1	,0172	,0914	,1887	,8504	-,1623	,1968
Int_1	,0482	,0619	,7783	,4368	-,0735	,1699

Product terms key:

Int_1 : Poz_apl x D1

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	,0005	,6058	1,0000	486,0000	,4368

Focal predict: Poz_apl (X)
Mod var: D1 (W)

Data for visualizing the conditional effect of the focal predictor:
Paste text below into a SPSS syntax window and execute to produce plot.

DATA LIST FREE/

Poz_apl D1 ketinim .
BEGIN DATA.

-1,4765	,0000	3,1142
,2735	,0000	4,4799
1,5235	,0000	5,4554
-1,4765	1,0000	3,0602
,2735	1,0000	4,5103
1,5235	1,0000	5,5460

END DATA.

GRAPH/SCATTERPLOT=

Poz_apl WITH ketinim BY D1 .

***** ANALYSIS NOTES AND ERRORS *****

Level of confidence for all confidence intervals in output:
95,0000

NOTE: The following variables were mean centered prior to analysis:
Poz_apl

----- END MATRIX -----

11 priedas

Požiūrio į aplikaciją bei ketinimo ją įsdiegti moderacija aplikacijos kategorijos atžvilgiu.

Run MATRIX procedure:

***** PROCESS Procedure for SPSS Version 4.0 *****

Written by Andrew F. Hayes, Ph.D. www.afhayes.com
Documentation available in Hayes (2022). www.guilford.com/p/hayes3

Model : 1
Y : ketinim
X : Poz_apl
W : APLIKAC

Sample
Size: 490

OUTCOME VARIABLE:
ketinim

Model Summary

	R	R-sq	MSE	F	df1	df2	p
	,7640	,5838	1,0179	227,2028	3,0000	486,0000	,0000

Model

	coeff	se	t	p	LLCI	ULCI
constant	4,0441	,1441	28,0580	,0000	3,7609	4,3273
Poz_apl	,7760	,0982	7,9017	,0000	,5831	,9690
APLIKAC	,1535	,0912	1,6842	,0928	-,0256	,3326
Int_1	,0179	,0617	,2911	,7711	-,1032	,1391

Product terms key:

Int_1 : Poz_apl x APLIKAC

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	,0001	,0848	1,0000	486,0000	,7711

Focal predict: Poz_apl (X)
Mod var: APLIKAC (W)

Data for visualizing the conditional effect of the focal predictor:
Paste text below into a SPSS syntax window and execute to produce plot.

DATA LIST FREE/

Poz_apl APLIKAC ketinim .
BEGIN DATA.

```

-1,4765      1,0000      3,0253
,2735        1,0000      4,4147
1,5235        1,0000      5,4072
-1,4765      2,0000      3,1523
,2735        2,0000      4,5732
1,5235        2,0000      5,5881
END DATA.
GRAPH/SCATTERPLOT=
  Poz_apl WITH      ketinim BY      APLIKAC .

***** ANALYSIS NOTES AND ERRORS *****

Level of confidence for all confidence intervals in output:
  95,0000

NOTE: The following variables were mean centered prior to analysis:
  Poz_apl

----- END MATRIX -----

```

12 priedas

H3 T testo rezultatai

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Suv_riz	3,7020	490	1,52849	,06905
	Pasitik	4,2176	490	1,34985	,06098

Paired Samples Test

		Paired Differences							
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference		t	df	Sig. (2-tailed)
					Lower	Upper			
Pair 1	Suv riz - Pasitik	-.51551	2.65901	.12012	-.75153	-.27949	-4.292	489	.000

13 priedas

H1 Stjudento T-testo rezultatai

Group Statistics

	POLITIKA	N	Mean	Std. Deviation	Std. Error Mean
Suv_riz	VIZU	245	3,3973	1,52983	,09774
	NEVIZ	245	4,0068	1,46807	,09379

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means					
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference
Suv_riz	Equal variances assumed	,461	,497	-4,500	488	,000	-,60952	,13546	-,87568 - ,34337
	Equal variances not assumed			-4,500	487,174	,000	-,60952	,13546	-,87568 - ,34337

14 priedas

H2 Stjudento T-testo rezultatai

Group Statistics					
	POLITIKA	N	Mean	Std. Deviation	Std. Error Mean
Pasitik	VIZU	245	4,5265	1,31778	,08419
	NEVIZ	245	3,9086	1,31279	,08387

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						95% Confidence Interval of the Difference
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Pasitik	Equal variances assumed	,134	,714	5,200	488	,000	,61796	,11884	,38446	,85145
	Equal variances not assumed			5,200	487,993	,000	,61796	,11884	,38446	,85145

15 priedas

H4 Stjudento T-testo rezultatai

Group Statistics					
	APSAUGA	N	Mean	Std. Deviation	Std. Error Mean
Poz_apl	TEIG	245	5,4184	1,24547	,07957
	NEIG	245	4,0347	1,37130	,08761

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						95% Confidence Interval of the Difference
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Poz_apl	Equal variances assumed	5,407	,020	11,691	488	,000	1,38367	,11835	1,15113	1,61621
	Equal variances not assumed			11,691	483,549	,000	1,38367	,11835	1,15113	1,61622

16 priedas

1 teiginio Westin indekso T-testo rezultatai lyties ir amžiaus atžvilgiu

	Lytis	Imtis	Vidurkis	Standartinis nuokrypis	Stand. klaidos reikšmė
WESTIN_1(R)	moteris	248	4,15	1,658	,105
	vyras	242	3,92	1,591	,102

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
WESTIN_1r	Equal variances assumed	,044	,833	1,551	488	,122	,228	,147	-,061	,516
	Equal variances not assumed			1,552	487,871	,121	,228	,147	-,061	,516

Group Statistics

	kateg	N	Mean	Std. Deviation	Std. Error Mean
WESTIN_1r	I kategorija	368	4,05	1,591	,083
	II kategorija	112	3,95	1,734	,164

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
WESTIN_1r	Equal variances assumed	2,329	,128	,584	478	,559	,102	,175	-,242	,447
	Equal variances not assumed			,558	171,780	,577	,102	,184	-,260	,465

17 priedas

2 teiginio Westin indekso T-testo rezultatai lyties ir amžiaus atžvilgiu

Group Statistics

	kateg	N	Mean	Std. Deviation	Std. Error Mean
WESTIN2	I kategorija	368	4,16	1,387	,072
	II kategorija	112	4,34	1,486	,140

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
WESTIN2	Equal variances assumed	1,742	,187	-1,158	478	,248	-,176	,152	-,475	,123
	Equal variances not assumed			-1,116	173,986	,266	-,176	,158	-,488	,135

Group Statistics

	Lytis	N	Mean	Std. Deviation	Std. Error Mean
WESTIN2	moteris	248	4,10	1,427	,091
	vyras	242	4,36	1,405	,090

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
WESTIN2	Equal variances assumed	,231	,631	-2,022	488	,044	-,259	,128	-,510	-,007
	Equal variances not assumed			-2,022	487,961	,044	-,259	,128	-,510	-,007

18 priedas

3 teiginio Westin indekso T-testo rezultatai lyties ir amžiaus atžvilgiu

Group Statistics

	Lytis	N	Mean	Std. Deviation	Std. Error Mean
WESTIN3	moteris	248	4,38	1,504	,095
	vyras	242	4,42	1,325	,085

Independent Samples Test

		Levene's Test for Equality of Variances					t-test for Equality of Means			95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference		Lower	Upper
WESTIN3	Equal variances assumed	5,716	,017	-,331	488	,741	-,042	,128		-,294	,209
	Equal variances not assumed			-,332	483,025	,740	-,042	,128		-,294	,209

Group Statistics

	kateg	N	Mean	Std. Deviation	Std. Error Mean
WESTIN3	I kategorija	368	4,30	1,379	,072
	II kategorija	112	4,59	1,492	,141

Independent Samples Test

		Levene's Test for Equality of Variances					t-test for Equality of Means			95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference		Lower	Upper
WESTIN3	Equal variances assumed	4,075	,044	-1,878	478	,061	-,285	,152		-,583	,013
	Equal variances not assumed			-1,801	172,688	,074	-,285	,158		-,597	,027

19 priedas

Faktorinė ANOVA vertinant privatumo politikos pranešimo formatų svarbą

Between-Subjects Factors

	Value Label	N
APLIKAC	1 UTI	245
	2 HED	245
POLITIKA	1 VIZU	245
	2 NEVIZ	245

Descriptive Statistics

Dependent Variable: Vizual

APLIKAC	POLITIKA	Mean	Std. Deviation	N
UTI	VIZU	5,5736	1,10295	111
	NEVIZ	4,1816	1,43510	134
	Total	4,8122	1,46735	245
HED	VIZU	5,5323	1,21335	134
	NEVIZ	4,0841	1,38058	111
	Total	4,8762	1,47770	245
Total	VIZU	5,5510	1,16247	245
	NEVIZ	4,1374	1,40863	245
	Total	4,8442	1,47138	490

Tests of Between-Subjects Effects

Dependent Variable: Vizual

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Noncent. Parameter	Observed Power ^b
Corrected Model	245,470 ^a	3	81,823	48,901	,000	146,703	1,000
Intercept	11391,008	1	11391,008	6807,757	,000	6807,757	1,000
APLIKAC	,584	1	,584	,349	,555	,349	,091
POLITIKA	244,873	1	244,873	146,347	,000	146,347	1,000
APLIKAC * POLITIKA	,096	1	,096	,057	,811	,057	,057
Error	813,194	486	1,673				
Total	12557,222	490					
Corrected Total	1058,664	489					

a. R Squared = ,232 (Adjusted R Squared = ,227)

b. Computed using alpha = ,05

Estimates

Dependent Variable: Vizual

APLIKAC	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
UTI	4,878	,083	4,714	5,041
HED	4,808	,083	4,645	4,971

Pairwise Comparisons

Dependent Variable: Vizual

(I) APLIKAC	(J) APLIKAC	Mean Difference (I-J)	Std. Error	Sig. ^a	95% Confidence Interval for Difference ^a	
					Lower Bound	Upper Bound
UTI	HED	,069	,117	,555	-,161	,300
HED	UTI	-,069	,117	,555	-,300	,161

Based on estimated marginal means

a. Adjustment for multiple comparisons: Bonferroni.

Univariate Tests

Dependent Variable: Vizual

	Sum of Squares	df	Mean Square	F	Sig.	Noncent. Parameter	Observed Power ^a
Contrast	,584	1	,584	,349	,555	,349	,091
Error	813,194	486	1,673				

The F tests the effect of APLIKAC. This test is based on the linearly independent pairwise comparisons among the estimated marginal means.

a. Computed using alpha = ,05

Estimates

Dependent Variable: Vizual

POLITIKA	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
VIZU	5,553	,083	5,390	5,716
NEVIZ	4,133	,083	3,970	4,296

Pairwise Comparisons

Dependent Variable: Vizual

(I) POLITIKA	(J) POLITIKA	Mean Difference (I-J)	Std. Error	Sig. ^b	95% Confidence Interval for Difference ^b	
					Lower Bound	Upper Bound
VIZU	NEVIZ	1,420 [*]	,117	,000	1,189	1,651
NEVIZ	VIZU	-1,420 [*]	,117	,000	-1,651	-1,189

Based on estimated marginal means

*. The mean difference is significant at the ,05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Univariate Tests

Dependent Variable: Vizual

	Sum of Squares	df	Mean Square	F	Sig.	Noncent. Parameter	Observed Power ^a
Contrast	244,873	1	244,873	146,347	,000	146,347	1,000
Error	813,194	486	1,673				

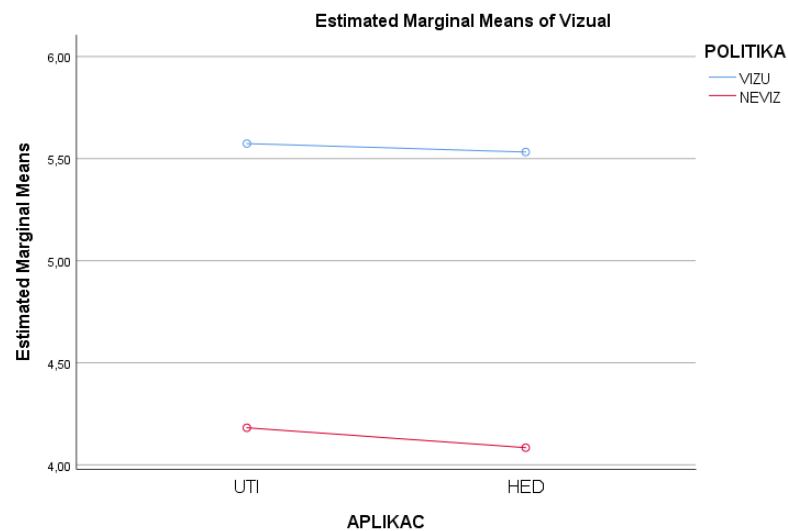
The F tests the effect of POLITIKA. This test is based on the linearly independent pairwise comparisons among the estimated marginal means.

a. Computed using alpha = ,05

3. APLIKAC * POLITIKA

Dependent Variable: Vizual

APLIKAC	POLITIKA	Mean	Std. Error	95% Confidence Interval	
				Lower Bound	Upper Bound
UTI	VIZU	5,574	,123	5,332	5,815
	NEVIZ	4,182	,112	3,962	4,401
HED	VIZU	5,532	,112	5,313	5,752
	NEVIZ	4,084	,123	3,843	4,325



20 priedas

Faktorinė ANOVA vertinant suvokiamą riziką esant skirtingiems privatumo politikos pranešimo rizikos lygmenims ir aplikacijos tipui

Between-Subjects Factors

		Value Label	N
APLIKAC	1	UTI	245
	2	HED	245
APSAUGA	1	TEIG	245
	2	NEIG	245

Descriptive Statistics

Dependent Variable: Suv_riz

APLIKAC	APSAUGA	Mean	Std. Deviation	N
UTI	TEIG	2,9617	1,22302	122
	NEIG	4,3889	1,52404	123
	Total	3,6782	1,55382	245
HED	TEIG	3,0271	1,30753	123
	NEIG	4,4303	1,36024	122
	Total	3,7259	1,50553	245
Total	TEIG	2,9946	1,26398	245
	NEIG	4,4095	1,44199	245
	Total	3,7020	1,52849	490

Tests of Between-Subjects Effects

Dependent Variable: Suv_riz

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Noncent. Parameter	Observed Power ^b
Corrected Model	245,628 ^a	3	81,876	44,370	,000	133,110	1,000
Intercept	6715,302	1	6715,302	3639,142	,000	3639,142	1,000
APLIKAC	,349	1	,349	,189	,664	,189	,072
APSAUGA	245,332	1	245,332	132,950	,000	132,950	1,000
APLIKAC * APSAUGA	,018	1	,018	,009	,922	,009	,051
Error	896,815	486	1,845				
Total	7857,944	490					
Corrected Total	1142,442	489					

a. R Squared = ,215 (Adjusted R Squared = ,210)

b. Computed using alpha = ,05

Estimates

Dependent Variable: Suv_riz

APLIKAC	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
UTI	3,675	,087	3,505	3,846
HED	3,729	,087	3,558	3,899

Pairwise Comparisons

Dependent Variable: Suv_riz

(I) APLIKAC	(J) APLIKAC	Mean Difference (I-J)	Std. Error	Sig. ^a	95% Confidence Interval for Difference ^a	
					Lower Bound	Upper Bound
UTI	HED	-,053	,123	,664	-,295	,188
HED	UTI	,053	,123	,664	-,188	,295

Based on estimated marginal means

a. Adjustment for multiple comparisons: Bonferroni.

Univariate Tests

Dependent Variable: Suv_riz

	Sum of Squares	df	Mean Square	F	Sig.	Noncent. Parameter	Observed Power ^a
Contrast	,349	1	,349	,189	,664	,189	,072
Error	896,815	486	1,845				

The F tests the effect of APLIKAC. This test is based on the linearly independent pairwise comparisons among the estimated marginal means.

a. Computed using alpha = ,05

Estimates

Dependent Variable: Suv_riz

APSAUGA	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
TEIG	2,994	,087	2,824	3,165
NEIG	4,410	,087	4,239	4,580

Pairwise Comparisons

Dependent Variable: Suv_riz

(I) APSAUGA	(J) APSAUGA	Mean Difference (I-J)	Std. Error	Sig. ^b	95% Confidence Interval for Difference ^b	
					Lower Bound	Upper Bound
TEIG	NEIG	-1,415 [*]	,123	,000	-1,656	-1,174
NEIG	TEIG	1,415 [*]	,123	,000	1,174	1,656

Based on estimated marginal means

*. The mean difference is significant at the ,05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Univariate Tests

Dependent Variable: Suv_riz

	Sum of Squares	df	Mean Square	F	Sig.	Noncent. Parameter	Observed Power ^a
Contrast	245,332	1	245,332	132,950	,000	132,950	1,000
Error	896,815	486	1,845				

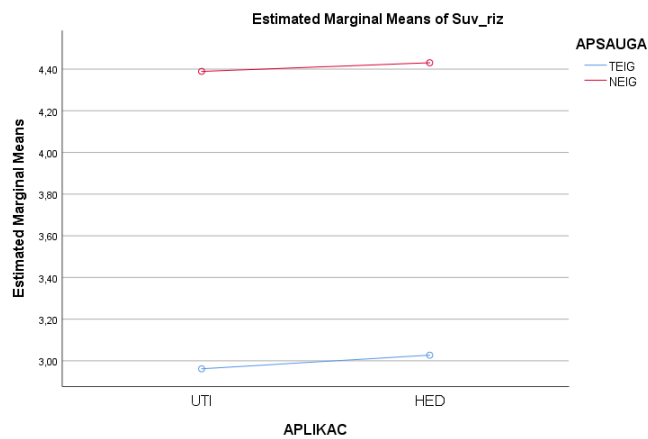
The F tests the effect of APSAUGA. This test is based on the linearly independent pairwise comparisons among the estimated marginal means.

a. Computed using alpha = ,05

3. APLIKAC * APSAUGA

Dependent Variable: Suv_riz

APLIKAC	APSAUGA	Mean	Std. Error	95% Confidence Interval	
				Lower Bound	Upper Bound
UTI	TEIG	2,962	,123	2,720	3,203
	NEIG	4,389	,122	4,148	4,630
HED	TEIG	3,027	,122	2,786	3,268
	NEIG	4,430	,123	4,189	4,672



21 priedas

Faktorinė ANOVA vertinant suvokiamą pasitikėjimą esant skirtingiems privatumo politikos pranešimo rizikos lygmenims ir aplikacijos tipui

Between-Subjects Factors			
		Value Label	N
APLIKAC	1	UTI	245
	2	HED	245
APSAUGA	1	TEIG	245
	2	NEIG	245

Descriptive Statistics				
Dependent Variable: Pasitik				
APLIKAC	APSAUGA	Mean	Std. Deviation	N
UTI	TEIG	4,8623	1,15511	122
	NEIG	3,6813	1,28620	123
	Total	4,2694	1,35607	245
HED	TEIG	4,7138	1,18601	123
	NEIG	3,6131	1,27006	122
	Total	4,1657	1,34438	245
Total	TEIG	4,7878	1,17069	245
	NEIG	3,6473	1,27603	245
	Total	4,2176	1,34985	490

Tests of Between-Subjects Effects

Dependent Variable: Pasitik

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Noncent. Parameter	Observed Power ^b
Corrected Model	160,950 ^a	3	53,650	35,715	,000	107,144	1,000
Intercept	8716,184	1	8716,184	5802,360	,000	5802,360	1,000
APLIKAC	1,438	1	1,438	,957	,328	,957	,164
APSAUGA	159,436	1	159,436	106,136	,000	106,136	1,000
APLIKAC * APSAUGA	,197	1	,197	,131	,717	,131	,065
Error	730,059	486	1,502				
Total	9607,000	490					
Corrected Total	891,009	489					

a. R Squared = ,181 (Adjusted R Squared = ,176)

b. Computed using alpha = ,05

Estimates

Dependent Variable: Pasitik

APLIKAC	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
UTI	4,272	,078	4,118	4,426
HED	4,163	,078	4,010	4,317

Pairwise Comparisons

Dependent Variable: Pasitik

(I) APLIKAC	(J) APLIKAC	Mean Difference (I-J)	Std. Error	Sig. ^a	95% Confidence Interval for Difference ^a	
					Lower Bound	Upper Bound
UTI	HED	,108	,111	,328	-,109	,326
HED	UTI	-,108	,111	,328	-,326	,109

Based on estimated marginal means

a. Adjustment for multiple comparisons: Bonferroni.

Univariate Tests

Dependent Variable: Pasitik

	Sum of Squares	df	Mean Square	F	Sig.	Noncent. Parameter	Observed Power ^a
Contrast	1,438	1	1,438	,957	,328	,957	,164
Error	730,059	486	1,502				

The F tests the effect of APLIKAC. This test is based on the linearly independent pairwise comparisons among the estimated marginal means.

a. Computed using alpha = ,05

Estimates

Dependent Variable: Pasitik

APSAUGA	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
TEIG	4,788	,078	4,634	4,942
NEIG	3,647	,078	3,493	3,801

Pairwise Comparisons

Dependent Variable: Pasitik

(I) APSAUGA	(J) APSAUGA	Mean Difference (I-J)	Std. Error	Sig. ^b	95% Confidence Interval for Difference ^b	
					Lower Bound	Upper Bound
TEIG	NEIG	1,141 [*]	,111	,000	,923	1,358
NEIG	TEIG	-1,141 [*]	,111	,000	-1,358	-,923

Based on estimated marginal means

*. The mean difference is significant at the ,05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Univariate Tests

Dependent Variable: Pasitik

	Sum of Squares	df	Mean Square	F	Sig.	Noncent. Parameter	Observed Power ^a
Contrast	159,436	1	159,436	106,136	,000	106,136	1,000
Error	730,059	486	1,502				

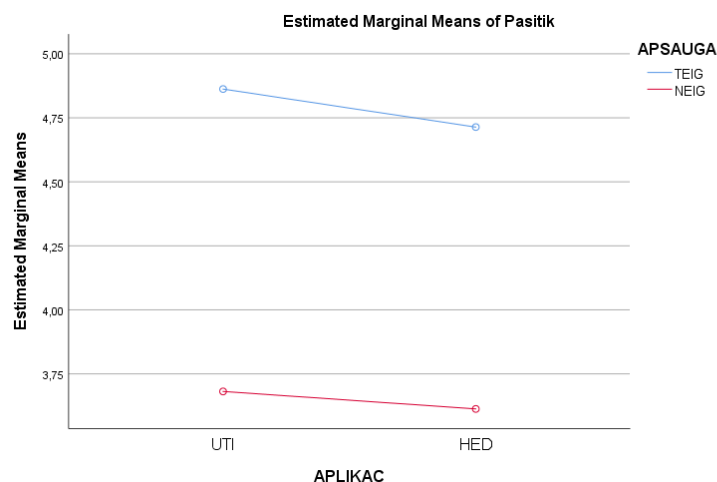
The F tests the effect of APSAUGA. This test is based on the linearly independent pairwise comparisons among the estimated marginal means.

a. Computed using alpha = ,05

3. APLIKAC * APSAUGA

Dependent Variable: Pasitik

APLIKAC	APSAUGA	Mean	Std. Error	95% Confidence Interval	
				Lower Bound	Upper Bound
UTI	TEIG	4,862	,111	4,644	5,080
	NEIG	3,681	,111	3,464	3,898
HED	TEIG	4,714	,111	4,497	4,931
	NEIG	3,613	,111	3,395	3,831



22 priedas

Empirinio tyrimo anketos

Aneka Nr.1

Gerbiami respondentai,

esu Vilniaus universiteto Verslo mokyklos skaitmeninės rinkodaros magistrantūros studentė. Šiuo metu rengiu magistro baigiamąjį darbą, todėl šia apklausa bus siekiama išsiaiškinti, kaip privatumo politikos

pateikimo būdai veikia apsisprendimą įsidiegti mobiliąsias aplikacijas (angl. Apps).

Apklausa yra anoniminė. Gauti atsakymai bus panaudoti tik akademiniams tikslams. Pildant apklausą užtruksite iki 10 minučių.

Dėkoju Jums.

Pažymėkite, kaip sutinkate su žemiau pateiktais teiginiais. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku - 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
Vartotojai prarado bet kokią kontrolę dėl įmonės renkamų duomenų ir asmeninės informacijos naudojimo	☐	☐	☐	☐	☐	☐	☐
Daugelis įmonių tinkamai ir konfidencialiai tvarko asmeninę informaciją, kurią renka apie vartotojus	☐	☐	☐	☐	☐	☐	☐
Galiojantys įstatymai ir organizacinė praktika užtikrina pagrįstą vartotojų privatumo apsaugos lygį šiandien.	☐	☐	☐	☐	☐	☐	☐

SITUACIJA 1A. Įsivaizduokite, kad svarstote įsidiegti MOBILIOSIOS BANKININKYSTĖS mobiliąją aplikaciją. Prieš įsidiegiant aplikaciją, Jūs esate supažindinamas (-a) su žemiau pavaizduota situacija:



[illegible]

Prisiminkite anksčiau pateiktą situaciją. Nurodykite, kaip sutinkate su žemiau pateiktais teiginiais, susijusiais su požiūriu į šią MOBILIOSIOS BANKININKYSTĖS aplikaciją. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku – 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
Manau, kad pateiktas privatumo pranešimas padėjo man suprasti galimas grėsmes, su kuriomis galiu susidurti							
Manau, kad pateiktas privatumo pranešimas buvo lengvai skaitomas							
Manau, kad pateiktas privatumo pranešimas buvo lengvai suprantamas							

Prisiminkite aukščiau pateiktą situaciją. Norėtumėme sužinoti Jūsų požiūrį ir ketinimą įsidedti šią MOBILIOSIOS BANKININKYSTĖS aplikaciją. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku - 1, visiškai sutinku – 7.

[illegible]

Aš ketinčiau įsidiesti šią aplikaciją	☐	☐	☐	☐	☐	☐	☐
Tikėtina, kad naudočiau šią aplikaciją, kai ji man bus reikalinga	☐	☐	☐	☐	☐	☐	☐
Manau, kad rekomenduočiau šią aplikaciją savo draugams.	☐	☐	☐	☐	☐	☐	☐

SITUACIJA 1B. Įsivaizduokite, kad svarstote įsidiesti SOCIALINIŲ TINKLŲ mobiliąją aplikaciją. Prieš įsidiegiant aplikaciją, Jūs esate supažindinamas (-a) su žemiau pavaizduota situacija:



[illegible]

	1	2	3	4	5	6	7
Manau, kad šī aplikacija perduos asmenīgu informāciju be mano leidimo							

man rasti galimas grėsmes, su kuriomis galiu susidurti							
Manau, kad pateiktas privatumo pranešimas buvo lengvai skaitomas	☐	☐	☐	☐	☐	☐	☐
Manau, kad pateiktas privatumo pranešimas buvo lengvai suprantamas	☐	☐	☐	☐	☐	☐	☐

Prisiminkite aukščiau pateiktą situaciją. Norėtumėme sužinoti Jūsų požiūrį ir ketinimą įsidiesti šią SOCIALINIŲ TINKLŲ aplikaciją. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku - 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
Jei turėsiu galimybę, naudosisiu šia aplikacija	☐	☐	☐	☐	☐	☐	☐
Manau, kad svarstyčiau įsidiesti šią aplikaciją	☐	☐	☐	☐	☐	☐	☐
Aš ketinčiau įsidiesti šią aplikaciją	☐	☐	☐	☐	☐	☐	☐
Tikėtina, kad naudočiau šią aplikaciją, kai ji man bus reikalinga	☐	☐	☐	☐	☐	☐	☐
Manau, kad rekomenduočiau šią aplikaciją savo draugams.	☐	☐	☐	☐	☐	☐	☐

Jūsų lytis:

1. Moteris
2. Vyras

Jūsų amžius (jau suėję metai):

Anketa Nr. 2

Gerbiami respondentai,

esu Vilniaus universiteto Verslo mokyklos skaitmeninės rinkodaros magistrantūros studentė. Šiuo metu rengiu magistro baigiamąjį darbą, todėl šia apklausa bus siekiama išsiaiškinti, kaip privatumo politikos pateikimo būdai veikia apsisprendimą įsidiesti mobiliąsias aplikacijas (angl. Apps).

Apklausa yra anoniminė. Gauti atsakymai bus panaudoti tik akademiniams tikslams. Pildant apklausą užtruksite iki 10 minučių.

Dėkoju Jums.

Pažymėkite, kaip sutinkate su žemiau pateiktais teiginiais. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku - 1, visiškai sutinku - 7.

	1	2	3	4	5	6	7
Vartotojai prarado bet kokią kontrolę dėl įmonės renkamų duomenų ir asmeninės informacijos naudojimo	☐	☐	☐	☐	☐	☐	☐
Daugelis įmonių tinkamai ir konfidencialiai tvarko asmeninę informaciją, kurią renka apie vartotojus	☐	☐	☐	☐	☐	☐	☐
Galiojantys įstatymai ir organizacinė praktika užtikrina pagrįstą vartotojų privatumo apsaugos lygį šiandien.	☐	☐	☐	☐	☐	☐	☐

SITUACIJA 2A. Įsivaizduokite, kad svarstote įsidiegti MOBILIOSIOS BANKININKYSTĖS mobiliąją aplikaciją. Prieš įsidiegiant aplikaciją, Jūs esate supažindinamas (-a) su žemiau pavaizduota situacija:

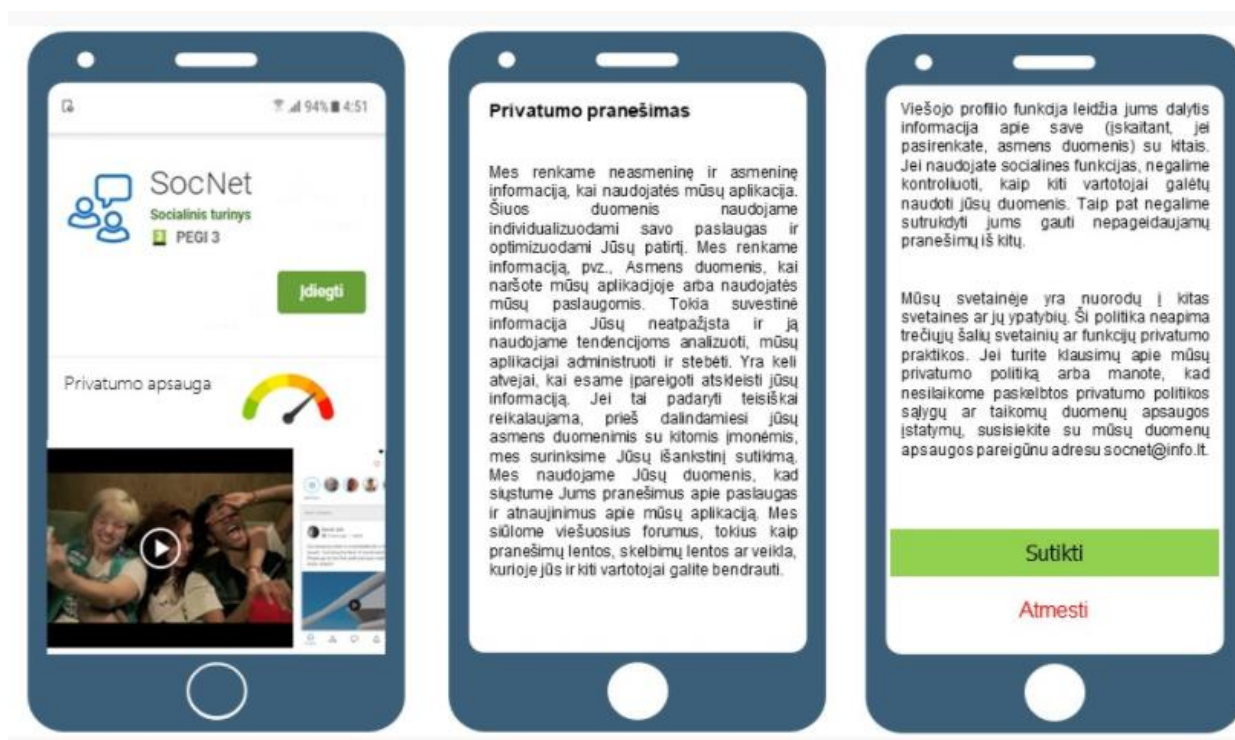


Manau, kad pateiktas privatumo pranešimas buvo lengvai skaitomas	☐	☐	☐	☐	☐	☐	☐
Manau, kad pateiktas privatumo pranešimas buvo lengvai suprantamas	☐	☐	☐	☐	☐	☐	☐

Prisiminkite aukščiau pateiktą situaciją. Norėtumėme sužinoti Jūsų požiūrį ir ketinimą įsidiesti šią MOBILIOSIOS BANKININKYSTĖS aplikaciją. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku - 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
Jei turėsiu galimybę, naudosisiu šia aplikacija	☐	☐	☐	☐	☐	☐	☐
Manau, kad svarstyčiau įsidiesti šią aplikaciją	☐	☐	☐	☐	☐	☐	☐
Aš ketinčiau įsidiesti šią aplikaciją	☐	☐	☐	☐	☐	☐	☐
Tikėtina, kad naudočiau šią aplikaciją, kai ji man bus reikalinga	☐	☐	☐	☐	☐	☐	☐
Manau, kad rekomenduočiau šią aplikaciją savo draugams.	☐	☐	☐	☐	☐	☐	☐

SITUACIJA 2B. Įsivaizduokite, kad svarstote įsidiesti SOCIALINIŲ TINKLŲ mobiliąją aplikaciją. Prieš įsidiegiant aplikaciją, Jūs esate supažindinamas (-a) su žemiau pavaizduota situacija:



Prisiminkite anksčiau pateiktą situaciją. Nurodykite, kaip sutinkate su žemiau pateiktais teiginiais, susijusiais su požiūriu į šią SOCIALINIŲ TINKLŲ aplikaciją. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku – 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
Mano požiūris į šią aplikaciją yra teigiamas	☐	☐	☐	☐	☐	☐	☐
Manau, kad ši aplikacija patenkins mano lūkesčius	☐	☐	☐	☐	☐	☐	☐
Mano požiūris į šią aplikaciją yra priimtinas	☐	☐	☐	☐	☐	☐	☐
Mano požiūris į šią aplikaciją yra malonus	☐	☐	☐	☐	☐	☐	☐

Prisiminkite anksčiau pateiktą situaciją. Nurodykite, kaip sutinkate su žemiau pateiktais teiginiais, susijusiais su SOCIALINIŲ TINKLŲ aplikacija. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku – 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
Manau, kad ši aplikacija perduos asmeninę informaciją be mano leidimo	☐	☐	☐	☐	☐	☐	☐
Manau, kad ši aplikacija gali pakenkti mano privatumui	☐	☐	☐	☐	☐	☐	☐
Manau, kad asmeninės informacijos pateikimas šiai aplikacijai galėtų sukelti daug neaiškumų	☐	☐	☐	☐	☐	☐	☐
Manau, kad susidurčiau su daugeliu problemų, pateikęs (-usi) savo asmeninę informaciją šiai aplikacijai	☐	☐	☐	☐	☐	☐	☐
Pateikti asmeninę informaciją šiai programai būtų rizikinga	☐	☐	☐	☐	☐	☐	☐
Manau, kad asmeninės informacijos pateikimas šiai aplikacijai sukeltų daug galimų nuostolių	☐	☐	☐	☐	☐	☐	☐

Prisiminkite anksčiau pateiktą situaciją. Nurodykite, kaip sutinkate su žemiau pateiktais teiginiais, susijusiais su šia SOCIALINIŲ TINKLŲ aplikacija. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku – 1, visiškai sutinku – 7.

Manau, kad rekomenduočiau šią aplikaciją savo draugams.	☐	☐	☐	☐	☐	☐	☐
---	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

Jūsų lytis:

1. Moteris
2. Vyras

Jūsų amžius (jau suėję metai):

Anketa Nr. 3

Gerbiami respondentai,

esu Vilniaus universiteto Verslo mokyklos skaitmeninės rinkodaros magistrantūros studentė. Šiuo metu rengiu magistro baigiamąjį darbą, todėl šia apklausa bus siekiama išsiaiškinti, kaip privatumo politikos pateikimo būdai veikia apsisprendimą įsidiegti mobiliąsias aplikacijas (angl. Apps).

Apklausa yra anoniminė. Gauti atsakymai bus panaudoti tik akademiniams tikslams. Pildant apklausą užtruksite iki 10 minučių.

Dėkoju Jums.

Pažymėkite, kaip sutinkate su žemiau pateiktais teiginiais. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku - 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
Vartotojai prarado bet kokią kontrolę dėl įmonės renkamų duomenų ir asmeninės informacijos naudojimo	☐	☐	☐	☐	☐	☐	☐
Daugelis įmonių tinkamai ir konfidencialiai tvarko asmeninę informaciją, kurią renka apie vartotojus	☐	☐	☐	☐	☐	☐	☐
Galiojantys įstatymai ir organizacinė praktika užtikrina pagrįstą vartotojų privatumo apsaugos lygį šiandien.	☐	☐	☐	☐	☐	☐	☐

SITUACIJA 3A. Įsivaizduokite, kad svarstote įsidiegti MOBILIOSIOS BANKININKYSTĖS mobiliąją aplikaciją. Prieš įsidiegiant aplikaciją, Jūs esate supažindinamas (-a) su žemiau pavaizduota situacija:

interesu							
Šios aplikacijos kūrėjai yra nuspėjami ir nuoseklūs informacijos naudojimo atžvilgiu	☐	☐	☐	☐	☐	☐	☐
Šios aplikacijos kūrėjai visada sąžiningai elgtųsi su klientais, kai reiktų naudoti mano pateiktą informaciją	☐	☐	☐	☐	☐	☐	☐

Prisiminkite anksčiau pateiktą situaciją. Nurodykite, kaip sutinkate su žemiau pateiktais teiginiais, susijusiais su požiūriu į šią MOBILIOSIOS BANKININKYSTĖS aplikaciją. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku – 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
Manau, kad vizualizuotas aplikacijos privatumo pranešimas padėjo man rasti galimas grėsmes, su kuriomis galiu susidurti	☐	☐	☐	☐	☐	☐	☐
Manau, kad pateiktas privatumo pranešimas buvo lengvai skaitomas	☐	☐	☐	☐	☐	☐	☐
Manau, kad pateiktas privatumo pranešimas buvo lengvai suprantamas	☐	☐	☐	☐	☐	☐	☐

Prisiminkite aukščiau pateiktą situaciją. Norėtumėme sužinoti Jūsų požiūrį ir ketinimą įsidiesti į šią MOBILIOSIOS BANKININKYSTĖS aplikaciją. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku - 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
Jei turėsiu galimybę, naudosisiu šia aplikacija	☐	☐	☐	☐	☐	☐	☐
Manau, kad svarstyčiau įsidiesti į šią aplikaciją	☐	☐	☐	☐	☐	☐	☐
Aš ketinčiau įsidiesti į šią aplikaciją	☐	☐	☐	☐	☐	☐	☐
Tikėtina, kad naudočiau šią aplikaciją, kai ji man bus reikalinga	☐	☐	☐	☐	☐	☐	☐
Manau, kad rekomenduočiau šią aplikaciją savo draugams.	☐	☐	☐	☐	☐	☐	☐

SITUACIJA 3B. Įsivaizduokite, kad svarstote įsidiesti SOCIALINIŲ TINKLŲ mobiliąją aplikaciją. Prieš įsidięiant aplikaciją, Jūs esate supažindinamas (-a) su žemiau pavaizduota situacija:

[illegible]

	1	2	3	4	5	6	7
Manau, kad šī aplikacija perduos asmenīgu informāciju be mano leiduma							

Manau, kad ši aplikacija gali pakenkti mano privatumui	☐	☐	☐	☐	☐	☐	☐
Manau, kad asmeninės informacijos pateikimas šiai aplikacijai galėtų sukelti daug neaiškumų	☐	☐	☐	☐	☐	☐	☐
Manau, kad susidurčiau su daugeliu problemų, pateikęs (-usi) savo asmeninę informaciją šiai aplikacijai	☐	☐	☐	☐	☐	☐	☐
Pateikti asmeninę informaciją šiai programai būtų rizikinga	☐	☐	☐	☐	☐	☐	☐
Manau, kad asmeninės informacijos pateikimas šiai aplikacijai sukeltų daug galimų nuostolių	☐	☐	☐	☐	☐	☐	☐

Prisiminkite anksčiau pateiktą situaciją. Nurodykite, kaip sutinkate su žemiau pateiktais teiginiais, susijusiais su SOCIALINIŲ TINKLŲ aplikacija. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku – 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
Šios aplikacijos kūrėjai būtų patikimi tvarkydami mano informaciją	☐	☐	☐	☐	☐	☐	☐
Šios aplikacijos kūrėjai pasakytų tiesą ir vykdytų pažadus susijusius su mano pateikta informacija	☐	☐	☐	☐	☐	☐	☐
Tikiu, kad šios aplikacijos kūrėjai tvarkydami informaciją, nepamirštų mano interesų	☐	☐	☐	☐	☐	☐	☐
Šios aplikacijos kūrėjai yra nuspėjami ir nuoseklūs informacijos naudojimo atžvilgiu	☐	☐	☐	☐	☐	☐	☐
Šios aplikacijos kūrėjai visada sąžiningai elgtųsi su klientais, kai reiktų naudoti mano pateiktą informaciją	☐	☐	☐	☐	☐	☐	☐

Prisiminkite anksčiau pateiktą situaciją. Nurodykite, kaip sutinkate su žemiau pateiktais teiginiais, susijusiais su požiūriu į šią SOCIALINIŲ TINKLŲ aplikaciją. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku – 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
--	---	---	---	---	---	---	---

Manau, kad pateiktas privatumo pranešimas padėjo man suprasti galimas grėsmes, su kuriomis galiu susidurti	☐	☐	☐	☐	☐	☐	☐
Manau, kad pateiktas privatumo pranešimas buvo lengvai skaitomas	☐	☐	☐	☐	☐	☐	☐
Manau, kad pateiktas privatumo pranešimas buvo lengvai suprantamas	☐	☐	☐	☐	☐	☐	☐

Prisiminkite aukščiau pateiktą situaciją. Norėtumėme sužinoti Jūsų požiūrį ir ketinimą įsdiegti šią SOCIALINIŲ TINKLŲ aplikaciją. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku - 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
Jei turėsiu galimybę, naudosisiu šia aplikacija	☐	☐	☐	☐	☐	☐	☐
Manau, kad svarstyčiau įsdiegti šią aplikaciją	☐	☐	☐	☐	☐	☐	☐
Aš ketinčiau įsdiegti šią aplikaciją	☐	☐	☐	☐	☐	☐	☐
Tikėtina, kad naudočiau šią aplikaciją, kai ji man bus reikalinga	☐	☐	☐	☐	☐	☐	☐
Manau, kad rekomenduočiau šią aplikaciją savo draugams.	☐	☐	☐	☐	☐	☐	☐

Jūsų lytis:

1. Moteris
2. Vyras

Jūsų amžius (jau suėję metai):

Anketa Nr. 4

Gerbiami respondentai,

esu Vilniaus universiteto Verslo mokyklos skaitmeninės rinkodaros magistrantūros studentė. Šiuo metu rengiu magistro baigiamąjį darbą, todėl šia apklausa bus siekiama išsiaiškinti, kaip privatumo politikos pateikimo būdai veikia apsisprendimą įsdiegti mobiliąsias aplikacijas (angl. Apps).

Apklausa yra anoniminė. Gauti atsakymai bus panaudoti tik akademiniams tikslams. Pildant apklausą užtruksite iki 10 minučių.

Dėkoju Jums.

Pažymėkite, kaip sutinkate su žemiau pateiktais teiginiais. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku - 1, visiškai sutinku - 7.

	1	2	3	4	5	6	7
Vartotojai prarado bet kokią kontrolę dėl įmonės renkamų duomenų ir asmeninės informacijos naudojimo	☐	☐	☐	☐	☐	☐	☐
Daugelis įmonių tinkamai ir konfidencialiai tvarko asmeninę informaciją, kurią renka apie vartotojus	☐	☐	☐	☐	☐	☐	☐
Galiojantys įstatymai ir organizacinė praktika užtikrina pagrįstą vartotojų privatumo apsaugos lygį šiandien.	☐	☐	☐	☐	☐	☐	☐

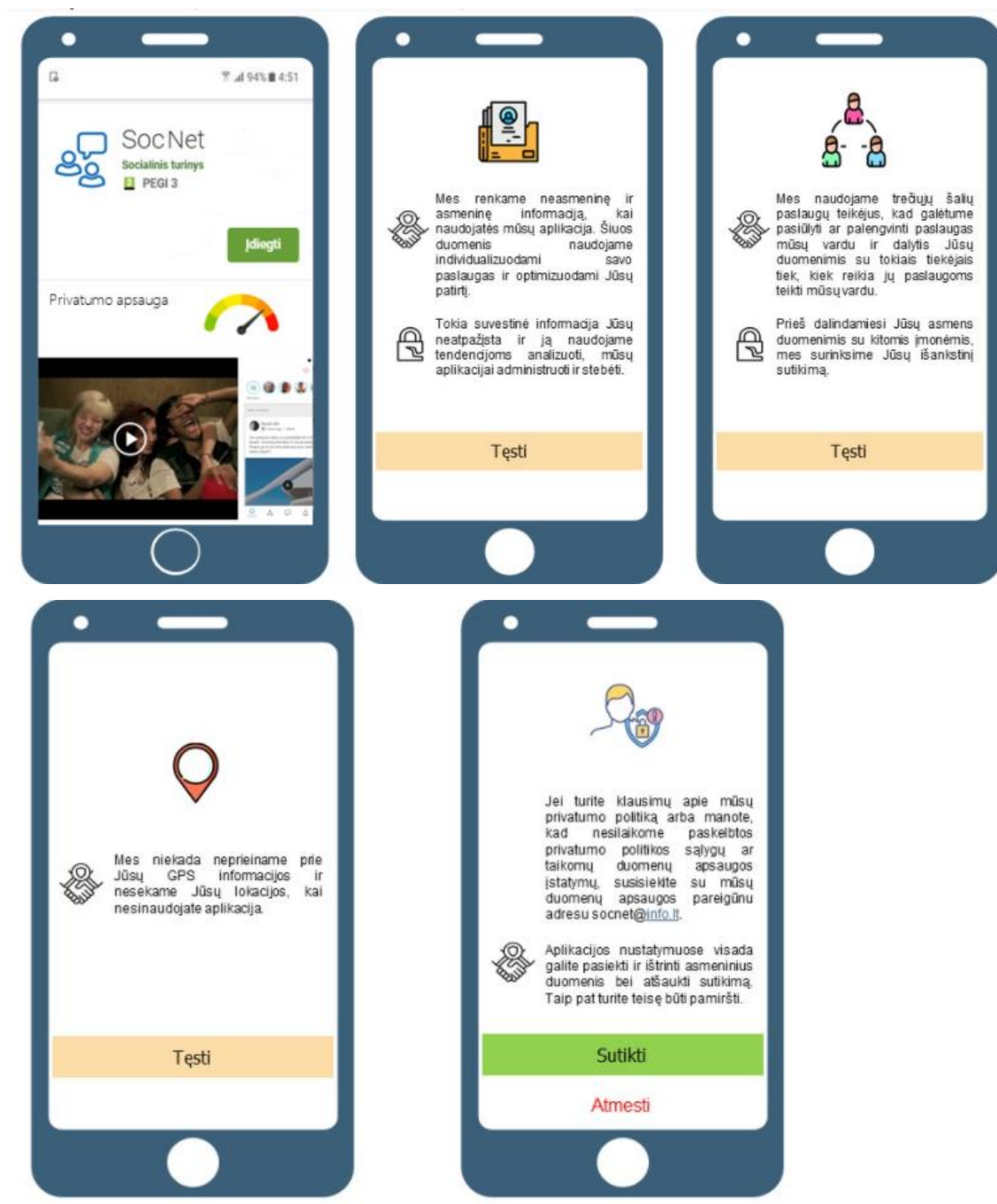
SITUACIJA 4A. Įsivaizduokite, kad svarstote įsidiegti MOBILIOSIOS BANKININKYSTĖS mobiliąją aplikaciją. Prieš įsidiegiant aplikaciją, Jūs esate supažindinamas (-a) su žemiau pavaizduota situacija:



Prisiminkite anksčiau pateiktą situaciją. Nurodykite, kaip sutinkate su žemiau pateiktais teiginiais, susijusiais su požiūriu į šią MOBILIOSIOS BANKININKYSTĖS aplikaciją. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku - 1, visiškai sutinku - 7.

Manau, kad rekomenduočiau šią aplikaciją savo draugams.	☐	☐	☐	☐	☐	☐	☐
---	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

SITUACIJA 4B. Įsivaizduokite, kad svarstote įsidięgti SOCIALINIŲ TINKLŲ mobiliąją aplikaciją. Prieš įsidięgiant aplikaciją, Jūs esate supažindinamas (-a) su žemiau pavaizduota situacija:



Prisiminkite anksčiau pateiktą situaciją. Nurodykite, kaip sutinkate su žemiau pateiktais teiginiais, susijusiais su požiūriu į šią SOCIALINIŲ TINKLŲ aplikaciją. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku – 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
Mano požiūris į šią aplikaciją yra teigiamas	☐	☐	☐	☐	☐	☐	☐
Manau, kad ši aplikacija patenkins mano lūkesčius	☐	☐	☐	☐	☐	☐	☐
Mano požiūris į šią aplikaciją yra priimtinas	☐	☐	☐	☐	☐	☐	☐
Mano požiūris į šią aplikaciją yra malonus	☐	☐	☐	☐	☐	☐	☐

Prisiminkite anksčiau pateiktą situaciją. Nurodykite, kaip sutinkate su žemiau pateiktais teiginiais, susijusiais su SOCIALINIŲ TINKLŲ aplikacija. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku – 1, visiškai sutinku – 7.

	1	2	3	4	5	6	7
Manau, kad ši aplikacija perduos asmeninę informaciją be mano leidimo	☐	☐	☐	☐	☐	☐	☐
Manau, kad ši aplikacija gali pakenkti mano privatumui	☐	☐	☐	☐	☐	☐	☐
Manau, kad asmeninės informacijos pateikimas šiai aplikacijai galėtų sukelti daug neaiškumų	☐	☐	☐	☐	☐	☐	☐
Manau, kad susidurčiau su daugeliu problemų, pateikęs (-usi) savo asmeninę informaciją šiai aplikacijai	☐	☐	☐	☐	☐	☐	☐
Pateikti asmeninę informaciją šiai programai būtų rizikinga	☐	☐	☐	☐	☐	☐	☐
Manau, kad asmeninės informacijos pateikimas šiai aplikacijai sukeltų daug galimų nuostolių	☐	☐	☐	☐	☐	☐	☐

Prisiminkite anksčiau pateiktą situaciją. Nurodykite, kaip sutinkate su žemiau pateiktais teiginiais, susijusiais su požiūriu į šią SOCIALINIŲ TINKLŲ aplikaciją. Kiekvienam teiginiui priskirkite reikšmę: visiškai nesutinku – 1, visiškai sutinku – 7.

Aš ketinčiau įsidiesti šią aplikaciją	☐	☐	☐	☐	☐	☐	☐
Tikėtina, kad naudočiau šią aplikaciją, kai ji man bus reikalinga	☐	☐	☐	☐	☐	☐	☐
Manau, kad rekomenduočiau šią aplikaciją savo draugams.	☐	☐	☐	☐	☐	☐	☐

Jūsų lytis:

1. Moteris
2. Vyras

Jūsų amžius (jau suėję metai):