

**VILNIAUS UNIVERSITETAS
KAUNO HUMANITARINIS FAKULTETAS**

INFORMATIKOS KATEDRA

Verslo informacijos sistemų studijų programa
kodas 62103S138

GINTA ŠOLYTĖ

MAGISTRO BAIGIAMASIS DARBAS

**PASITIKĖJIMO ELEMENTŲ ELEKTRONINIO BALSAVIMO
SISTEMOSE TYRIMAS**

Kaunas 2009

**VILNIAUS UNIVERSITETAS KAUNO
HUMANITARINIS FAKULTETAS
INFORMATIKOS KATEDRA**

GINTA ŠOLYTĖ

VERSLO INFORMACIJOS SISTEMŲ MAGISTRO STUDIJŲ PROGRAMA

Magistro baigiamasis darbas

**PASITIKĖJIMO ELEMENTŲ ELEKTRONINIO BALSAVIMO
SISTEMOSE TYRIMAS**

Leidžiama ginti _____

Magistrantas: _____

Darbo vadovas: Doc. Dr. D. Krikščiūnienė

(parašas) _____

Darbo _teikimo data _____

Registracijos Nr. _____

Darbo _vertinimas _____

(data, _vertinimas, komisijos pirmininko parašas)

Kaunas 2009

TURINYS

SANTRUMPŲ SAŽAŠAS	3
LENTELIŲ SAŽAŠAS	5
PAVEIKSLŲ SAŽAŠAS	6
SANTRAUKA	7
ĮVADAS	8
1. TEORINIS/ANALITINIS SKYRIUS	10
1.1 Pasitikėjimą el. valdžia nagrinėjančios literatūros analizė	10
1.3 El. balsavimo sistemų modeliai bei projektai	12
1.3.1 Teoriniai pasitikėjimo el. valdžia modeliai	13
1.3.2 Lietuvos elektroninio balsavimo sistemos koncepcija	16
1.3.3 Estijos elektroninio balsavimo sistemos projektas	19
1.3.4 Šveicarijos elektroninio balsavimo sistema.....	23
1.3.5 Europos tarybos ministrų komiteto požiūris į el. balsavimą	27
1.4 Pasitikėjimo el. balsavimo sistemomis veiksnių analizė	32
1.5 Teorinio skyriaus išvados	33
2. SIŪLOMO SPRENDIMO METODIKA.....	35
2.1 Rinkėjų pasitikėjimą lemiančių veiksnių analizė sistemose.....	35
2.2 Rinkėjų pasitikėjimą lemiantys veiksniai	38
2.3 Pasitikėjimą didinantis el. balsavimo sistemos modelis.....	40
2.4 Siūlomo sprendimo metodikos skyriaus išvados.....	43
3. EKSPERIMENTINIS SKYRIUS.....	44
3.1 Duomenų rinkimas	44
3.2 Tyrimo vieta, laikas, pradžios ir pabaigos datos	45
3.3 Tyrimo apribojimai.....	45
3.4 Duomenų apdorojimas ir analizė.....	45
3.5 Rezultatų analizė	46
3.6 Rezultatų interpretavimas ir apibendrinimas - Pakartotinio prisijungimo posistemė	59
3.6.1 Rinkėjo konfidencialumas	62
3.6.2 Valdžios institucija.....	65
3.6.3 Sistemos skaidrumas.....	65
3.6.4 Sistemos tikslumas	67
3.6.5 Pagalba	69
3.7 Eksperimentinio skyriaus išvados	73
IŠVADOS.....	74
Literatūra	77
PRIEDAI	80
1 PRIEDAS	80
2 PRIEDAS	86
3 PRIEDAS	92
Mokslo - tiriamojo darbo planas.....	98

SANTRUMPŲ SAŽAŠAS

BSA – balsus skaičiuojanti aplikacija.

BPS – balsus perduodantis serveris.

BSS – balsus skaičiuojantis serveris.

EBS - elektroninio balsavimo sistema.

El. balsadėžė – elektroninė balsadėžė.

El. balsas – elektroninis balsas.

El. balsavimas – elektroninis balsavimas naudojant šiuolaikines informacines sistemas. Šiame darbe naudojama sąvoka el balsavimas vartojama kaip santrumpa nuotolinio el. balsavimo, kuomet elektroninis balsavimas vykdomas naudojant šiuolaikines informacines sistemas ir balsuojant nuotoliniu būdu.

ES – Europos sąjunga.

El. valdžia – informacijos ir komunikacijos technologijų bei Interneto panaudojimas gerinant prieinamą prie valdžios paslaugų ir geresnę šių paslaugų pristatymą piliečiams, verslui, darbuotojams, ir kitiems dalyviams.

ID kortelė – identifikavimo kortelė.

IS - Informacinės sistemos.

KTU - Kauno Technologijos universitetas.

LRS – Lietuvos Respublikos Seimas.

MRU – Mykolo Riomerio universitetas.

TSPMI - Tarptautinių studijų politikos mokslo institutas.

VRK – Vyriausioji rinkimų komisija.

VU - Vilniaus universitetas.

VS – vartotojo sąsaja.

SSL (Secure Socket Layer) – rankų paspaudimo protokolas susidedantis iš dviejų dalių: serverio autentifikacijos ir kliento autentifikacijos.

LENTELIŲ SĄRAŠAS

1 lentelė. Pasitikėjimo el. valdžia faktoriai	16
2 lentelė. Bandomieji balsavimai Šveicarijoje	24
3 lentelė. Šveicarijos el. balsavimo sistemos ir balsavimo paštu palyginimas	25
4 lentelė. El. balsavimo sistemos saugumo aspektai.....	29
5 lentelė. Pasitikėjimui Lietuvos el. balsavimo sistema kylančios grėsmės	32
6 lentelė. Pasitikėjimui Estijos el. balsavimo sistema kylančios grėsmės	32
7 lentelė. Pasitikėjimui Šveicarijos el. balsavimo sistema kylančios grėsmės	33
8 lentelė. Pasitikėjimą lemiančių veiksnių el. balsavimo sistemose palyginimas.....	35
9 lentelė. Rodiklių, lemiančių pasitikėjimą el. balsavimo sistema pasiskirstymas.....	53

PAVEIKSLŲ SĄRAŠAS

1 pav.	Lietuvos elektroninio balsavimo sistemos veiksmų diagrama	18
2 pav.	Estijos el. balsavimo sistemos balsavimo metodas.	19
3 pav.	Estijos elektroninio balsavimo sistemos projekto architektūra.	20
4 pav.	Estijos el. balsavimo sistemos balsavimo proceso komponentai.	21
5 pav.	Balsų rūšiavimas ir atšaukimas Estijos el. balsavimo sistemoje	22
6 pav.	Balsų skaičiavimas Estijos el. balsavimo sistemoje	23
7 pav.	Pasitikėjimo el. balsavimo sistema elementai.	38
8 pav.	Pasitikėjimą didinantis el. balsavimo sistemos modelis	42
9 pav.	Respondentų pasiskirstymas pagal lytį.	46
10 pav.	Respondentų pasiskirstymas pagal amžių.	47
11 pav.	Respondentų pasiskirstymas pagal pastovią gyvenamąją vietą.	47
12 pav.	Respondentų pasiskirstymas pagal išsilavinimą	48
13 pav.	Respondentų pasiskirstymas pagal naudojimosi kompiuteriu lygį	48
14 pav.	Respondentų pasiskirstymas pagal naudojamą el. valdžios paslaugomis.	49
15 pav.	Pasiskirstymas pagal naudojamą skirtingomis el. valdžios paslaugomis.	49
16 pav.	Pasiskirstymas pagal balsavimo būdus	50
17 pav.	Pasiskirstymas pagal el. balsavimo reikalingumą respondentų šalyse.	50
18 pav.	Priežastys dėl kurių el. balsavimas turėtų būti įdiegtas.	51
19 pav.	Tinkamiausias sistemos kūrėjas bei palaikytojas.	52
20 pav.	Išankstinis apklaustųjų pasitikėjimas el. balsavimo sistema.	52
21 pav.	Pasitikėjimas valdžia bei rinkimais.	53
22 pav.	Pasitikėjimo elementai autentifikacijos procese	54
23 pav.	Patvirtinimo apie balso užregistravimą reikalingumas.	54
24 pav.	Patvirtinimo būdai, kad balso užregistruotas balsavimo procese.	55
25 pav.	Saugaus ryšio kanalo naudojimo balso perdavimui svarbumas.	55
26 pav.	Balso užšifravimas perdavimo metu saugiu kriptografiniu metodu	56
27 pav.	Galimybės parsisiųsti nemokamą antivirusinę programą ir perskanuoti kompiuterį	56
28 pav.	Sistemos audito svarbumas.	57
29 pav.	Pagalbos įrankiai, įtakojantys rinkėjo pasitikėjimą el. balsavimo sistema.	57
30 pav.	Sistemoje realizuoto balsų perskaičiavimo svarbumas	58
31 pav.	Svarbumas, kad rinkimų balsai nebūtų paviešinti prieš rinkimų pabaigą.	58
32 pav.	Kompetingų rinkimų komisijos atstovų dalyvavimas balsų skaičiavime	59
33 pav.	Balsavimo etapai.	60
34 pav.	Pakartotinio prisijungimo langas.	61
35 pav.	Rinkėjo balso statuso istorija	62
36 pav.	Balsų nuo rinkėjų ID atskyrimas	63
37 pav.	Balsavimo procesas iki balsų atskyrimo.	64
38 pav.	Patvirtinimas apie balso užregistravimą	66
39 pav.	Pakartotinis prisijungimas prie sistemos.	67
40 pav.	Autentifikacijos procesas el. balsavimo sistemoje	68
41 pav.	Asmeninė autentifikacijos istorija.	69
42 pav.	Pagalbų rūšys	70
43 pav.	Online pagalba	70
44 pav.	Pagalba telefonu.	71
45 pav.	Pagalba naudojant DUK.	71
46 pav.	Demo versija.	72

SANTRAUKA

ŠOLYTĖ, Ginta. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas. MBA Graduation Paper. Kaunas: Vilnius University, Kaunas Faculty of Humanities, Department of Informatics.98 p.

S U M M A R Y

The purpose of this research is to find out trust elements in e-voting systems and possible ways of implementation of them in IS. The objects of research are theoretical Lithuanian e-voting system's concept and Geneva's e-Voting, Estonian I-Voting systems. The main tasks were performed in order to solve this research problem: theoretical trust in e-government models were analysed, the research of trust elements in Lithuanian e-voting system's concept and Geneva's e-Voting, Estonian I-Voting systems were done, complex trust model in e-voting were described and finally the experiment was done. Methods used in research – analysis of scientific literature, the complex trust in e-voting model is created in order to find out it's validity, experiment consisting of questionnaire is made. The results and conclusions of research – after analysis of trust models in e-government we concluded that these factors can be divided into two groups - pre-interactional factors: individual citizen, institutional attributes, technology and interactional factors: product/service attributes, transactional delivery and fulfilment of services and information content attributes. After analysis of Lithuanian e-voting system's concept and Geneva's e-Voting, Estonian I-Voting systems trust elements were defined. The experiment – a questionnaire gave results that the most important factors while creating e-voting systems in order to stimulate citizens trust are citizens confidentiality, trust in government, system's visibility – confirmation of vote have been registered, system's accuracy – safe authentication and wide selection of help services. Pages in total: 68, sum of tables: 9, sum of pictures: 46.

ĮVADAS

Šiame darbe sprendžiamos **problemos aktualumas**: Lietuvoje yra kuriama sistema, kuri įgyvendins el. balsavimą pagal "Balsavimo internetu rinkimuose ir referendume koncepciją". Tačiau sistemos diegimo aplinka (situacija Lietuvoje) ir priimta koncepcija neužtikrina nei specialistų, nei Lietuvos piliečių pasitikėjimo ja. Lyginant ES ir Lietuvoje diegiamas elektroninio balsavimo sistemas, matomas technologinis skirtumas tarp jų, tačiau pasitikėjimo jomis problema išlieka. Būtina išsiaiškinti pasitikėjimą lemiančius elementus sistemose ne tik iš technologinės, bet ir socialinės bei ekonominės pusės.

Atliekamo darbo **mokslinė problema** - kokie faktoriai lemia pasitikėjimą el. balsavimo sistemomis? **Problemoms ištyrimo lygis** visame pasaulyje skiriasi dėl susidomėjimo pačiomis sistemomis ir atliekamų darbų šia linkme. Atlikti darbai vertina pasitikėjimą el. valdžia: McKnight D.H. Choudhury V., Kacmar, C. (2002); Tassabehji R., Elliman T. (2006); Teo T.S.H. (2008). Taip pat atlikta darbų tiriančių el. balsavimo sistemų saugumo reikalavimus bei sistemos kūrimo nuostatus: Magi T. (2007); Republique et Cantonde Geneve. (2007); Ramonaitė A. (2008). Tačiau nagrinėjant literatūrą darbų tiesiogiai tiriančių faktorius lemiančius pasitikėjimą el. balsavimo sistemomis nebuvo rasta.

Darbo objektas - teorinės bei realizuotos el. balsavimo sistemos: Lietuvos el. balsavimo teorinis modelis, Estijos bei Šveicarijos el. balsavimo sistemos. Darbe siekiama **tikslo** - ištirti pasitikėjimo elementus el. balsavimo sistemose ir jų įdiegimo IS prielaidas. Siekiant iškelto tikslo, yra sprendžiami šie pagrindiniai **darbo uždaviniai**: 1) išanalizuoti teorinius modelius, kurie nagrinėja pasitikėjimą el. valdžia. 2) išnagrinėti esamose elektroninio balsavimo sistemose Estijoje bei Šveicarijoje ir Lietuvos teoriniame modelyje, egzistuojančius pasitikėjimą kuriančius elementus. 3) pasiūlyti specializuotą apimantį tiek technologinius, tiek socialinius, ekonominius aspektus; pasitikėjimą elektroninėmis balsavimo sistemomis kuriantį modelį. 4) atlikti eksperimentinį tyrimą ir įvertinti pasiūlyto metodo taikymo galimybes.

Darbo struktūra susideda iš pagrindinių dalių: įvado, kuriame aptariamas darbo objektas – el. balsavimo sistemos; tikslo, kuriuo siekiama ištirti el. balsavimo sistemų pasitikėjimo veiksnius ir jų įdiegimo IS prielaidas bei iškeltų uždavinių: išanalizuoti teorinius modelius, kurie nagrinėja pasitikėjimą el. valdžia, išnagrinėti esamose elektroninio balsavimo sistemose egzistuojančius pasitikėjimą kuriančius elementus, pasiūlyti specializuotą pasitikėjimą elektroninėmis balsavimo sistemomis kuriantį modelį bei atlikti eksperimentinį tyrimą ir įvertinti pasiūlyto metodo taikymo galimybes. Teorinis skyrius nagrinėja teorinius pasitikėjimą el. valdžia kuriančius modelius bei realias elektroninio balsavimo sistemas. Siūlomo sprendimo metodika - mokslinės literatūros

analizė ir egzistuojančių elektroninio balsavimo sistemų analizė, siekiant nustatyti pasitikėjimo elementus el. balsavimo sistemose. Antroje dalyje, pateikiama preliminarus siūlomos elektroninės balsavimo sistemos koncepcijos tyrimas. Eksperimentinis skyrius aprašo duomenų rinkimą, jų apdorojimą bei analizę. Aprašoma atlikta apklausa, kurios metu buvo tikrinamas pasiūlyto modelio veiksmingumas. Taip pat atliekama rezultatų analizė, interpretavimas, apibendrinimas bei išvados.

Darbe naudoti literatūros šaltiniai: teorinius el. valdžia pasitikėjimo elementus nagrinėjantys autoriai. Žymiausi iš jų: McKnight D.H. Choudhury V., Kacmar, C. (2002); Tassabehji R., Elliman T. (2006); Teo T.S.H. (2008). Estijos el. balsavimo sistemą nagrinėjantys autoriai: Magi T. (2007); The National Election Committee. (2005). Šveicarijos el. balsavimo sistemą nagrinėjantys autoriai: Federal Office of Communications OFCOM. (2007). Taip pat analizuojant naudotasi tiriamaisiais darbais atliktais įvertinti el. balsavimo sistemos diegimo galimybes Lietuvoje: Ramonaitė A. (2008) bei LRS priimtais įstatymais. Šaltinių rūšys naudotos darbe: moksliniai straipsniai, magistro tezės, knygos, pranešimai seminaruose, analitinės studijos, įstatymai. Taip pat naudoti interneto šaltiniai, lyginant su moksline literatūra (17 šaltinių), jie sudarė mažesnę dalį (15 šaltinių).

Tyrimo metodai, kuriuos ketinama iširti ir panaudoti darbe: nagrinėjama mokslinė literatūra ir atliekama jos analizė bei apibendrinimas. Kuriamas eksperimentinis modelis patikrinti ar nustatyti veiksniai įtakoja pasitikėjimą sistemomis. Atliekamas kiekybinis tyrimas, anketiniu būdu bus tiriami piliečiai, siekiant nustatyti ar siūlomos pasitikėjimą kuriančios priemonės įtakoja jų pasirinkimą. **Darbo rezultatų teorinė ir praktinė reikšmė:** išanalizuoti teoriniai pasitikėjimo el. valdžia modeliai. Išnagrinėtos Šveicarijos bei Estijos el. balsavimo sistemos, apibendrinus Šveicarijos bei Estijos el. balsavimo sistemas bei atlikus teorinių modelių analizę buvo pasiūlytas pasitikėjimą el. balsavimo sistemomis kuriantis modelis. Jis apima devynis pagrindinius elementus, kurie remiantis atlikta analize turi įtakos rinkėjo pasitikėjimui. Pasitikėjimą kuriantys elementai: rinkėjo konfidencialumo užtikrinimas, pasitikėjimo valdžia kūrimas bei išlaikymas, sistemos skaidrumas – patvirtinimas apie balso užregistravimą bei pakartotinį prisijungimą, rinkimų tikslumas– ypatingai saugi autentifikacija, visapusiška pagalba vartotojui – online pagalba. Gauti rezultatai gali būti panaudoti praktiškai kuriant pasitikėjimą lemiančias el. balsavimo sistemas.

Rezultatų aprobavimas - parengtas straipsnis "Pasitikėjimo elementų el. balsavimo sistemose tyrimas" (Šolytė, G. (2009)). Straipsnio tekstas pateikiamas 3 priede.

Darbą sudaro trys pagrindinės dalys teorinis skyrius, siūlomo sprendimo metodika bei eksperimentinis skyrius. Iš viso 98 puslapiai, 9 lentelės, 46 paveikslai ir 3 priedai.

1. TEORINIS/ANALITINIS SKYRIUS

Šis skyrius skirtas teoriškai nagrinėti darbe keliamą problemą. Analizuojami teoriniai pasitikėjimo el. valdžia modeliai. Taip pat atliekama išsami Estijos bei Šveicarijos el. balsavimo sistemų analizė, tirama Lietuvos el. balsavimo koncepcija. Šios sistemos tiriamos kaip tyrimo srities objektas. Darbo tyrimo sritis apima sritį, kur valdžia susikerta su piliečiais ($C \leftrightarrow G$), vadinama El. valdžia, El. demokratija sritis (Sundgren, A., 2005, p.8). Siekiama išspręsti šiuos uždavinius: išanalizuoti teorinius modelius, kurie nagrinėja pasitikėjimą el. valdžia bei išnagrinėti esamose elektroninio balsavimo sistemose Estijoje bei Šveicarijoje ir Lietuvos teoriniame modelyje, egzistuojančius pasitikėjimą kuriančius elementus.

1.1 Pasitikėjimą el. valdžia nagrinėjančios literatūros analizė

Žymiausi autoriai: Johns, J.L. (1996) pasiūlė proceso – rezultatų pasitikėjimo modelį. Modelis susideda iš keturių lygių: informacijos asimiliacijos, sprendimų priėmimo, pasitikėjimo santykio bei pasitikėjimo pasekmių (Johns, J.L. (1996)). McKnight, D.H.; Choudhury, V.; Kacmar, C. (2002) siūlomas pasitikėjimo kūrimo modelis susideda iš pasitikėjimo intencijų ir pasitikėjimo įsitikinimų. Juos įtakoja puslapio reputacija, puslapio kokybė bei struktūriniai garantai (McKnight, D.H.; Choudhury, V.; Kacmar, C. (2002)). Teo, T.S.H (2008) teigia, kad santykių kokybė tarp tranzakcinių dalių veikia piliečių pasitikėjimą labiau nei technologinė sąsaja. Jis teigia, kad pasitikėjimas valdžia bei pasitikėjimas technologija tiesiogiai veikia pasitikėjimą el. valdžios paslaugomis (Teo, T.S.H (2008)). Apžvelgus autorių darbus galime teigti, kad jie nagrinėja pasitikėjimo el. valdžia kaip kompleksiską problemą. Šie darbai leidžia toliau nagrinėti bei tirti pasitikėjimo elementus el. balsavimo sistemose.

1.2 El. balsavimo sistemas nagrinėjančios literatūros analizė

Mokslinė literatūra šia tema buvo sugrupuota remiantis tematinio apjungimo principu. Išskiriamos trys pagrindinės sistemos, kurios atitinka darbo objektą – el. balsavimo sistemą. Svarbus darbas, nagrinėjantis Estijos el. balsavimo sistemą yra T. Magi darbas „Practical Security Analysis of E-voting Systems“. Jame nagrinėjami technologiniai aspektai, kurie lėmė Estijoje įdiegtos el. balsavimo sistemos pasisekimą. Darbe aprašomas pasirengimas balsavimui, ID kortelių projektas, viešojo rakto kriptografijos bei skaitmeninio parašo naudojimas (Magi, T., (2007)). The

National Election Committee. (2005)“ E-voting system overview“ aprašomas bei nagrinėjamas sistemos principinis veikimas, el. balsavimo etapai, sistemos architektūra ir dalyvaujantys asmenys bei el. balsavimo procedūros¹.

Reikšmingi darbai nagrinėjant Šveicarijos el. balsavimo sistemą yra Krimmer, R. (2006) darbas „Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed“ (Krimmer, R. (2006)). Darbe aptariama projekto situacija, rekomendacijos tolimesniems darbams. State Chancellery. (2007) „State Council’s Report to the Grand Council on the Geneva electronic voting project“ pranešimas išsamiai aprašo kaip buvo pasiruošta el. balsavimo sistemos įdiegimui šalyje, taip pat gaunama analizei naudinga informacija apie sistemos veikimą, jos aprašymas, infrastruktūra, saugumo aspektai, finansinė projekto pusė, atlikti testai bei auditai².

Svarbūs darbai nagrinėjantys Lietuvos el. balsavimo sistemą yra E. Dambausko straipsnis dėl LR Seimo nutarimo “Dėl balsavimo internetu rinkimuose ir referendumuose koncepcijos patvirtinimo”, kuris įvardina svarbiausius technologinius faktorius, kurie trukdo sistemai atitikti visus reikalingus technologinius kriterijus: rinkėjo identifikavimo problema, VRK serverio sertifikavimas, El. balsadėžės patikimumo patikrinimo galimybė³. „Elektroninio balsavimo galimybių studija“ darbe išskiriami elektroninio balsavimo sunkumai: galimos grėsmės Lietuvos politinės sistemos stabilumui ir valdžios legitimumui, jei kils techninių problemų arba jei vidinės ar išorinės jėgos sukels nepasitikėjimą sistema; grėsmė Lietuvos įvaizdžiui, jei rinkimai nebus sėkmingi arba jei žinia apie el. balsavimo įvedimą nebus tinkamai pristatyta; būtinybė atsisakyti balsavimo privatumo principo bei galimi kiti neigiami padariniai demokratijos kokybei (Ramonaitė, A. (2008)). LRS priimta “Balsavimo internetu rinkimuose ir referendumuose koncepcija”, kurioje nurodomi, kokie teisiniai dalykai yra dar neišspręsti ir kuriuos rodiklius sistema turi turėti norint įdiegti el. balsavimo sistemą Lietuvoje: rinkimų visuotinumą, el. balsavimo saugumą, slapto balsavimo principo laikymąsi, el. balsavimo sistemos prieinamumą, suprantamumą ir lengvą naudojimą, betarpiškumą tarp rinkėjo ir sistemos, teisės aktų neatitikimas⁴.

¹ The National Election Committee. (2005) E-voting system overview [interaktyvus]. Talinas: The National Election Committee

² State Chancellery. (2007) State Council’s Report to the Grand Council on the Geneva electronic voting project [interaktyvus]. Republic and Canton of Geneva: State Chancellery.

³ DAMBAUSKAS, E. (2007) Analitinė studija: Dėl LR Seimo nutarimo „Dėl balsavimo internetu rinkimuose ir referendumuose koncepcijos patvirtinimo“ [interaktyvus]. Vilnius: Viešojo įstaiga Demokratinės politikos institutas (DPI).

⁴ Lietuvos Respublikos Seimas. (2006) Balsavimo internetu rinkimuose ir referendumuose koncepcija [interaktyvus]. Vilnius: Lietuvos Respublikos Seimas

1.3 El. balsavimo sistemų modeliai bei projektai

El. balsavimo bandymų atlikta santykinai nedaug. Pirmieji bandymai Olandijoje nebuvo sėkmingi. 2004 m. vykusiuose Europos rinkimuose olandai, gyvenantys užsienyje galėjo balsuoti internetu. Sistemos KOA (Kiezen OpAfstand) ir RIES (Rijnland Internet Election System) buvo panaudotos rinkimuose⁵. JAV vykdytame SERVE projekte taip pat rasta daug saugumo spragų, kurios palieka galimybę atlikti kibernetines atakas prieš sistemą: atakas iš vidaus, automatiškus balsų pirkimo atvejus, virusų sukeltas atakas prieš vartotojo kompiuterį, kurios gali sukelti katastrofiškas pasekmes. Todėl šios sistemos buvo nuspręsta atsisakyti (David, J.; Rubin, A.D.; Barbara, S.; Wagner, D., (2004)). El. balsavimo bandymai yra taip pat įvykdyti Didžiojoje Britanijoje, Šveicarijoje, Ispanijoje, Prancūzijoje bei Estijoje. Šveicarijoje elektroninio balsavimo eksperimentai buvo įvykdyti trijuose kantonuose 2003 m., taip pat penki bandomieji balsavimai įvykdyti 2004 ir 2005 m. nacionaliniuose referendumuose Ženevos, Niurnbergo ir Ciuricho kantonuose. Iki šiol vienintelė šalis, įvedusi el. balsavimą rinkimuose nacionaliniu mastu, yra Estija. Estijoje el. balsavimas buvo panaudotas 2005 spalio mėn. savivaldos rinkimuose ir 2007 m. parlamento rinkimuose. Lietuvoje 2006 m. Lietuvos Respublikos Vyriausybės nutarime „Dėl Elektroninės valdžios koncepcijos įgyvendinimo priemonių plano patvirtinimo“ pakeitimo neįtraukė el. balsavimo sistemos į priemonių planą⁶, tačiau vėliau tais pačiais metais buvo priimta „Balsavimo internetu rinkimuose ir referendumuose koncepcija“, kuri apibrėžia teorinį būsimos sistemos modelį. Be to kaip rašoma A. Kačinskienės pranešime aktyviai vykdomi kiti el. valdžios paslaugų projektai: paraiškos, pajamų deklaravimas, laisvų darbo vietų paieška, transporto priemonių registravimas, kurie turėtų sudaryti sąlygas imtis svarbesnių tokių kaip el. balsavimo sistemos diegimo Lietuvoje projekto. Vyriausioji rinkimų komisija, (2007) paskelbė, kad konkursą laimėjo „Ernst & Young Baltic“ kompanija, be to buvo sudaryta darbo grupė Informacinės visuomenės plėtros komiteto prie LR Vyriausybės, Vyriausiosios rinkimų komisijos (VRK), Lietuvos banko, Krašto apsaugos ministerijos ir kitų institucijų atstovai. Kuriama sistema garantuoja visų rinkimų principų išsaugojimą^{7 8}.

⁵ KITCAT, J. (2007) Dutch voting computers decertified [interaktyvus]. Amsterdam: "Wij vertrouwen stemcomputers niet",

⁶ Lietuvos Respublikos Vyriausybė. (2006) Dėl Lietuvos Respublikos Vyriausybės 2003 m. lapkričio 25 d. Nutarimo nr. 1468 „Dėl Elektroninės valdžios koncepcijos įgyvendinimo priemonių plano patvirtinimo“ pakeitimo

⁷ Vyriausioji rinkimų komisija. (2007a) Elektroninio balsavimo sistemos kūrimo darbai įgyja pagreitį [interaktyvus]. Vilnius: Vyriausioji rinkimų komisija.

⁸ Vyriausioji rinkimų komisija. (2007b) Sėkmingai tęsiami internetinio balsavimo sistemos kūrimo darbai [interaktyvus]. Vilnius: Vyriausioji rinkimų komisija.

Prieš analizuojant sistemas, svarbu pagrįsti kodėl būtent šios dvi sistemos – Šveicarijos bei Estijos buvo pasirinktos kaip analizės objektai. 2003 m. ir 2005 m. Šveicarijos el. balsavimo sistema buvo finalistė ES organizuojamo konkurso “eEurope Awards”. Taip pat šis projektas buvo pristatytas kaip pavyzdinis Europos ministerinėse konferencijose skirtose IT, vykusioms 2003 m. liepos mėn. Como mieste, Italijoje, 2005 m. lapkričio mėn. Mančesteryje, Anglijoje. 2006 m. ši sistema buvo „Stockholm Challenge“, pasaulinio lygio IT aplikacijų konkurso finalistė. Šveicarijos administracinio mokslo draugija „Swiss society for administrative science” 2004 m. spalio mėn. Apdovanojo šią sistemą kaip multidisciplinę, technologiškai, socialiai, politiškai bei teisiškai veikiančią sistemą, kuri didelį dėmesį skiria piliečių informavimui bei abipusiškumui tarp valdžios ir jų palaikyti. 2007 m. Šveicarijos el. balsavimo sistema buvo Jungtinių Tautų viešųjų paslaugų apdovanojimų (United Nations Public Service) finalistė. Tais pačiais metais Europos el. valžios apdovanojimų „European eGovernment Awards“ konsorciumas apdovanojo sistemą Europos „Good Practice“ ženklu. Tuo tarpu 2007 m. Europos el. valžios apdovanojimų „European eGovernment Awards“ konsorciumas apdovanojo Estijos el. sistemą Europos „Good Practice“ ženklu. Be to kaip jau buvo minėta anksčiau, Estija vienintelė šalis, įvedusi internetinį balsavimą rinkimuose nacionaliniu mastu. Estijoje balsavimas internetu buvo panaudotas 2005 spalio mėn. savivaldos rinkimuose ir 2007 m. parlamento rinkimuose. Taip pat rengiamasi ja ir vėl naudotis 2009 m. vyksiančiuose rinkimuose. Lietuvos el. balsavimo sistemos koncepcija pasirinkta dėl problemos aktualumo bei rezultatų pritaikomumo atlikus šį mokslinį darbą.

1.3.1 Teoriniai pasitikėjimo el. valdžia modeliai

Pasitikėjimą labai sudėtinga išmatuoti tiesiogiai; „Paskutiniu metu jis išsivystė iš statistinės į dinamiškesnę koncepciją su skirtingais vystymosi etapais ar fazėmis bei skirtingomis charakteristikomis“ (Tassabehji, R.; Elliman, T. (2006), p.3). Siekiant sukurti pasitikėjimą el. valdžios paslaugomis, reikalinga suprasti faktorius, kurie įtakoja vartotojo pasitikėjimo formavimosi procesus.

Johns, J.L. (1996) pasiūlė proceso – rezultatų pasitikėjimo modelį. Vartotojai gauna informaciją iš dviejų šaltinių pasitikėjimo elemento (el. valdžios objekto) ir situacijos, apdoroja ją ir sukuria savo pasitikėjimą. Šis modelis aprašomas keturiais pagrindiniais lygiais:

- 1. Informacijos asimiliacija:** pasitikėjimo objekto bei situacinių faktorių suvokimas. Pasitikėjimo objekto aspektai - kompetencija, patikimumas ir atitinkama patirtis. Situaciniai faktoriai apima rizikos suvokimą būdinguose santykiuose ir potencialią naudą priimant riziką.

2. Sprendimų priėmimas: informacijos apdorojimas, pasitikėjimas patikimumu pasitikėjimo elementu. Vartotojas tikisi priimdamas sprendimą jam teigiamą rezultatą.
3. Pasitikėjimo santykis: jei potencialus pasitikėjimo objektas atrodo vertas pasitikėjimo atitinkamoje situacijoje, vartotojas pereis į pasitikėjimo santykį. Svarbu asmens nusiteikimas, santykis, pasikliovimas, asmenys, veikimas, lūkesčiai, procesas, dinamika, evoliucija ar vystymasis, rezultatai.
4. Pasitikėjimo pasekmės: realizacija laukto naudingumo, nenumatyti rezultatai ir stabilūs ar kintantys pasitikėjimo lygiai (Johns, J.L. (1996)).

McKnight, D.H.; Choudhury, V.; Kacmar, C. (2002) siūlomas pasitikėjimo kūrimo modelis susideda iš pasitikėjimo intencijų ir pasitikėjimo įsitikinimų – noro priklausyti nuo puslapio savininko. Juos įtakoja puslapio reputacija, puslapio kokybė bei struktūriniai garantai. Pasitikėjimas bei suvokta rizika veikia vartotojo elgesį. Pasitikėjimas užtikrina, kad vartotojai jaustųsi saugūs pateikdami savo asmeninę informaciją, kad naudotis internetu yra naudinga, kad yra saugu naudoti informaciją pateiktą internete (McKnight, D.H.; Choudhury, V.; Kacmar, C. (2002)).

Kim, D.J.; Song, Y. I.; Braynov, S.B.; Rao, H.R. (2005) sukurtas multidimensinis pasitikėjimo el. verslu modelis susideda iš stebinčio vartotojo, pasitikėjimą teikiančio objekto ir aplinkos (technologijų ir trečiosios šalies). Jis aprašomas šešiais pasitikėjimo lygiais:

1. Kliento-elgesio lygis – individualūs atributai, kurie veikia klientų pasitikėjimo elgesį. Tai yra demografiniai faktoriai, patirtis, susipažinimas su sistema, individuali kultūra, tradicijos, privatumas ir kt.
2. Institucinis lygis – trečiosios šalys ir kiti instituciniai faktoriai, kurie keičia institucinę aplinką. Tai yra reputacija, autentifikavimas, patvirtinimas, klientų bendruomenės bei įstatymai.
3. Informacinis lygis – savybės, nustatančios puslapio sandaros patikimumą: tikslumas, išbaigtumas, nešališkumas, patikimumas, autorinis puslapio ženklas, aplinka ir naudingumas.
4. Produkto lygis – produkto atributai, kurie traukia ar atstumia nuo mainų, vykstančių internetinėje erdvėje. Tai yra ilgaamžiškumas, kokybė, pritaikomumas individualiam klientui, konkurentiškumas ir prieinamumas.
5. Tranzakcijos lygis - atributai, paverčiantys internetu vykstančias tranzakcijas patikimomis. Tai yra skaidrumas, finansinis planavimas, su pardavimais susijusios paslaugos, pirkimo skatinimas bei pristatymas.
6. Technologinis lygis – IS bei programinės įrangos savybės, kurie įgalina internetu vykstančias tranzakcijas būti efektyvias bei saugias. Tai yra medijos perdavimo kokybė,

sąsajos dizainas ir sudėtis, saugumas, abipusiškumas, skaitmeninis sertifikatas, viešojo rakto infrastruktūra, autentiškumas, vientisumas, konfidencialumas, neanuliuotumas, kompetencija ir nuspėjamumas (Kim, D.J.; Song, Y. I.; Braynov, S.B.; Rao, H.R. (2005)).

Parent, M. (2006) įvardina pasitikėjimą valdžia mažinančius faktorius: visuomenės suvokimas apie neveiksmingumą, neefektyvumas ir politikos atitolimas nuo piliečių. Pasitikėjimą valdžia didina - padidėjęs veiksmingumas, skaidrumas, pasikeitimai, sąveika, antikorupcija, efektyvumas, ir politikos priartinimas prie piliečių (Parent, M. (2006)).

Teo, T.S.H (2008) teigia, kad santykių kokybė tarp tranzakcinių dalių veikia piliečių pasitikėjimą labiau nei technologinė sąsaja. Jis teigia, kad pasitikėjimas valdžia bei pasitikėjimas technologija tiesiogiai veikia pasitikėjimą el. valdžios paslaugomis. Pasitikėjimas el. valdžios paslaugomis, savo ruožtu, veikia: informacijos kokybę, sistemos bei paslaugų kokybę. Pasitikėjimas technologija: sistemos patikimumas, kompetencija ir saugumas, privatumo ir saugumo rizika. Pasitikėjimas ir kokybės suvokimas: asmeninės charakteristikos veikia asmens elgesį, jos susiformuoja su išankstiniu tikėjimu. Kokybės suvokimas: sąveikos suvokimas, sąveikos įvertinimas ir kokybės charakteristika. Suvokta kokybė – informacija, vartotojo sąsajos draugiškumas, adaptacija ir estetika. Pasitikėjimas ir informacijos kokybė: informacija turi būti tiksli, veiksminga ir pateikta laiku. Pasitikėjimas ir sistemos kokybė: piliečiai tiki, kad valdžios institucijos sugeba efektyviai adresuoti skirtingas technologines problemas sustiprinti vartojamumą. Pasitikėjimas ir paslaugos kokybė – jei piliečiai pasitiki el. valdžia jie bus linkę būti tolerantiškesni ir mažiau reikalaujantys. Ir pateisins neigiamą patirtį: tranzakcijų vėlavimą, prailgintą aplikacijos apdorojimo laiką (Teo, T.S.H (2008)).

Apžvelgus pasitikėjimą el. valdžia tiriančių autorių darbus, pasitikėjimą kuriančius faktorius galima suskirstyti į dvi grupes: prieš sąveiką su sistema ir sąveikos metu. Pasitikėjimo el. valdžia modelis susideda iš stebinčio vartotojo, pasitikėjimą teikiančio objekto ir aplinkos (technologijų ir trečiosios šalies). 1 lentelėje pateikiami sugrupuoti požymiai pagal požymių tipus.

Pasitikėjimo el. valdžia faktoriai

Veikimo laikas	Požymių tipas	Požymiai
Prieš sąveiką	Individualaus piliečio elgesio požymiai	Subjektyvios normos, individuali demografija, polinkis į el. valdžią, pažinimo procesas, bendros intencijos pasitikėjimui ir el. paslaugų naudojimas; kitų asmenų nuomonė, patirtis, susipažinimas su sistema, individuali kultūra bei tradicijos
	Instituciniai požymiai	Organizacijos reputacija, akreditacija, bendrai suvokiamas organizacijos patikimumas, autentifikavimas, vartotojų bendruomenės, įstatyminiai reikalavimai, autoritetas ir kompetencija.
	Technologiniai Požymiai	Perdavimo kokybė, sąsajos dizainas ir sudėtis, saugumas, abipusiškumas, skaitmeninis sertifikatas, viešojo rakto infrastruktūra, autentiškumas, vientisumas, struktūriniai garantai, neanuliuotumas, kompetencija ir nuspėjamumas, privatumas, tranzakcijos nuoseklumas, prieinamumas ir konfidencialumas
Sąveikos metu	Paslaugos požymiai	Ilgaamžiškumas, patikimumas, pritaikomumas individualiam vartotojui, prieinamumas ir kokybė: informacija, vartotojo sąsajos draugiškumas ir estetika.
	Tranzakcijos išpildymas	Skaidrumas, aptarnavimas po tranzakcijos įvykdymo, tikslumas ir kokybė.
	Informacijos savybės	Tikslumas, išbaigtumas, nešališkumas, patikimumas, aplinka, naudingumas ir kokybė.

Šaltinis: sudaryta autoriaus.

1.3.2 Lietuvos elektroninio balsavimo sistemos koncepcija

Remiantis atliktos Capgemini apklausos duomenimis Lietuva atsilieka nuo ES pasitenkinimo el. valdžia vidurkio (64%), tai yra 12% mažiau nei ES vidurkis. Taip pat Lietuva atsilieka teikdama kitas el. paslaugas⁹. Todėl svarbu tinkamai rengti el. valdžios projektus ir atsižvelgti į vartotojų poreikius. Dar 2005 m. Lietuvos Respublikos Vyriausios rinkimų komisijos pirmininko ataskaitoje buvo pažymima, kad el. balsavimas turėtų būti įdiegtas Lietuvoje dėl kelių svarbių priežasčių: rinkėjų migracijos, dažnai ne tik šalies viduje bet ir išvykstant į užsienį; visuomenės įpročio naudotis technologijų suteikiamomis galimybėmis paslaugas gauti ar užsisakyti neišeinant iš namų¹⁰. LRS 2006 m. priėmė „Balsavimo internetu rinkimuose ir referendumuose koncepcija“. Joje teigiama, kad kuriant el. balsavimo sistemą susiduriama su keliomis pagrindinėmis problemomis: rinkėjo identifikavimu, vieningos ir visiems prieinamos identifikacijos infrastruktūros nebuvimo, siūlomos el. bankininkystės naudojimu autentifikacijai ir su tuo susijusiu saugumu¹¹. Remiantis koncepcija balsavimas vyktų sekančia tvarka:

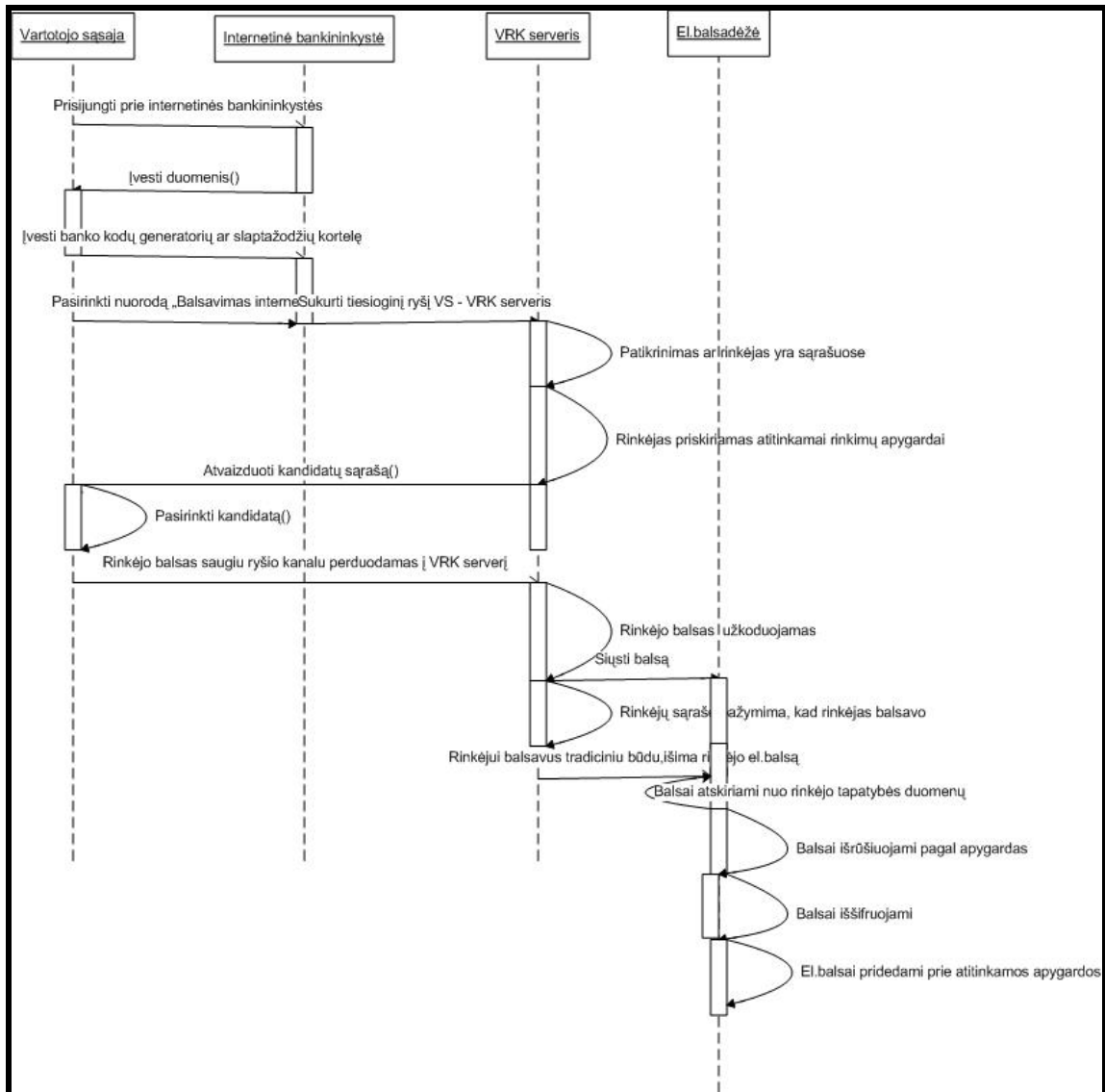
⁹ Capgemini. (2007) The User Challenge Benchmarking The Supply Of Online Public Services, 7th Measurement [interaktyvus]. Diegem (Belgium): Capgemini Belgium NV/SA.

¹⁰ VAIGAUSKAS, Z. (2006) Lietuvos Respublikos Seimui Lietuvos Respublikos Vyriausios rinkimų komisijos pirmininko ataskaita už 2005 metus.

¹¹ Lietuvos Respublikos Seimas. (2006) Balsavimo internetu rinkimuose ir referendumuose koncepcija [interaktyvus]. Vilnius: Lietuvos Respublikos Seimas.

1. Rinkėjas vienu iš galimų kanalų arba tiesiogiai prisijungia į VRK balsavimo tinklą, arba jungiasi prie savo el. bankininkystės sistemos.
2. Jei rinkėjas naudoja banko identifikavimo sistemą, įsijungęs į savo banko sąskaitos tvarkymo tinklą (naudodamas banko kodų generatorių ar slaptažodžių kortelę), jis pasirenka nuorodą „Balsavimas internetu“, ar pan., ir yra perkeliamas į VRK serverį. Kartu bankas perduoda VRK serveriui banko pasirašytą informaciją, apie prisijungusį rinkėją, o pats atsijungia iš ryšio grandinės, palikdamas tiesioginį ryšį „rinkėjas-VRK“.
3. VRK serveris, gavęs informaciją iš banko apie prisijungusį rinkėją, patikrina, ar toks rinkėjas yra rinkimų sąrašuose ir priskiria rinkėją atitinkamai rinkimų apygardai. Po patikrinimo, VRK sistema rinkėjo „paklausia“, ar tai tikrai tas rinkėjas, kuris prisistato.
4. Rinkėjui ekrane pateikiamas „el. biuletenis“, kuriame rinkėjas pažymi savo pasirinkimą (pasirinkimus) ir jį patvirtina. Informacija ekrane turi būti aiški, suprantama ir kiek įmanoma panaši į rinkėjams įprastą balsavimo apylinkėje ar paštu biuletenį.
5. Rinkėjo balsas saugiu ryšio kanalu perduodamas į VRK serverį, kur nedelsiant užkoduojamas ir patenka į elektroninę balsadėžę. Rinkėjų sąraše pažymima, kad rinkėjas balsavo, o užkoduotas balsas su rinkėjo identifikacijos duomenimis patenka į el. balsadėžę, kur yra saugomas iki tradicinio balsavimo pabaigos.
6. Rinkėjui nusprendus internetu pareikšti savo valią pakartotinai, procedūra pakartojama iš naujo, tačiau pirmiau priimtasis balsas išimamas iš el. balsadėžės ir į jo vietą įtraukiamas naujas.
7. Pasibaigus el. balsavimo laikui, el. balsadėžė „uždaroma“, t.y. atjungiamą nuo išorinio ryšio kanalų, o pagal internetu balsavusių asmenų sąrašą pažymimi rinkėjai rinkėjų sąrašuose, numatytuose skirstyti apygardoms ir apylinkėms.
8. Rinkėjui atvykus į rinkimų apylinkę rinkimų dieną ir balsavus tradiciniu būdu, rinkėjų sąrašuose (kuriuose apylinkės komisijos narys mato, kad rinkėjas balsavo internetu) pažymima, kad rinkėjas atvyko į apylinkę ir apie tai informuojama rinkimų apygarda, kuri, savo ruožtu, informuoja VRK serverį, kuris išima (anuliuoja) rinkėjo el. balsą.
9. Pasibaigus rinkimų dienai, biuletiniai ir paštu gauti vokai skaičiuojami įprasta tvarka, o VRK servery esantys balsai atskiriami nuo rinkėjo tapatybės duomenų, išrūšiuojami pagal apygardas ir iššifruojami, VRK surašomas el. balsavimo protokolas. El. balsadėžės balsai iššifruojami naudojant sudėtingą fragmentuotą šifrą, kurio skirtingus fragmentus turi skirtingi Vyriausiosios rinkimų komisijos nariai. Tik surinkus visą raktą galima iššifruoti el. balsadėžę.

Gavus apygardų rinkimų rezultatus, el. balsai pridedami prie atitinkamos apygardos ir skelbiami galutiniai rezultatai¹².



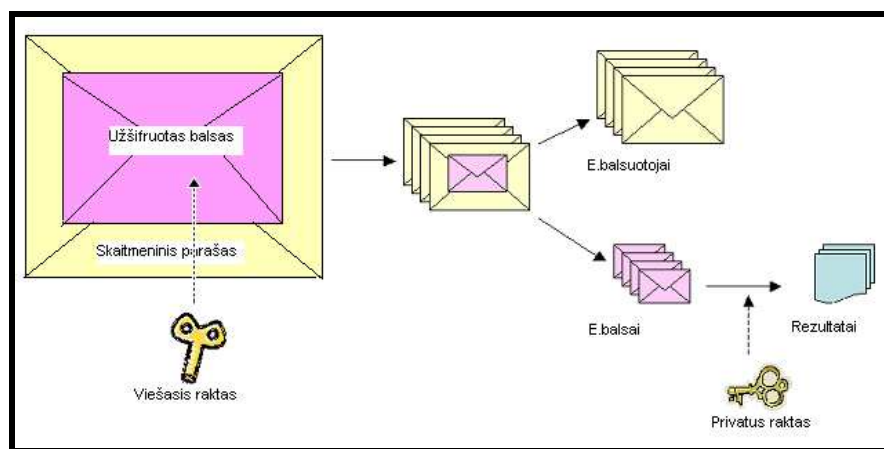
Šaltinis: sukurta autoriaus pagal LIETUVOS RESPUBLIKOS SEIMAS. (2006) Balsavimo internetu rinkimuose ir referendumuose koncepcija, p. 6-8.

1 pav. Lietuvos elektroninio balsavimo sistemos veiksmų diagrama.

¹² Lietuvos Respublikos Seimas. (2006) Balsavimo internetu rinkimuose ir referendumuose koncepcija [interaktyvus]. Vilnius: Lietuvos Respublikos Seimas.

1.3.3 Estijos elektroninio balsavimo sistemos projektas

Estijos el. balsavimo koncepcija yra panaši į balsavimą paštu. Estijoje sukurta el. balsavimo koncepcija pasižymi galimybe veikti kartu su tradiciniais rinkimais, sistemos paprastumu – minimaliu komponentų ir dalių skaičiumi ir visišku SP panaudojimu¹³. Taip pat ji pasižymi didele skvarba, daugiau nei 850,000 žmonių turi ID kortelę, tai reiškia, kad dauguma turinčių teisę balsuoti asmenų (1,06 mln. Populiacija) turi galimybę pasinaudoti el. balsavimo sistema¹⁴. 2 pav. pavaizduotas Estijos el. balsavimo sistemos balsavimo metodas.



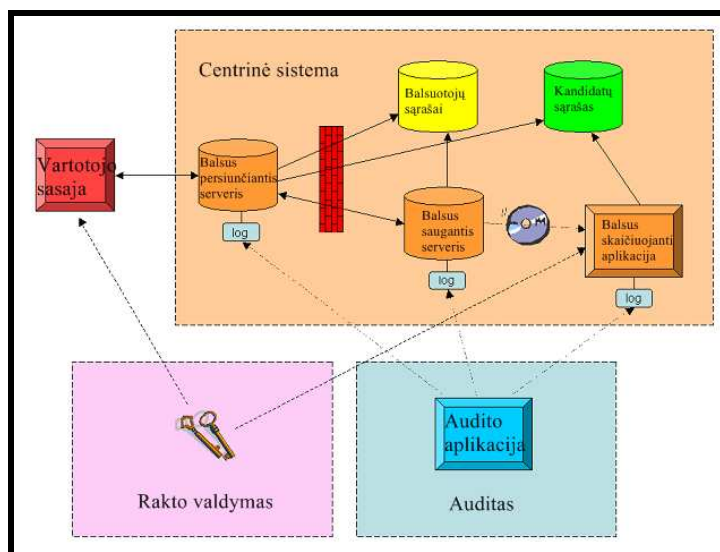
Šaltinis: THE NATIONAL ELECTION COMMITTEE. (2005) E-voting system overview, p. 8.

2 pav. Estijos el. balsavimo sistemos balsavimo metodas.

Estijos el. balsavimo sistemos projekto architektūra ir dalyvaujančios dalys pavaizduoti 3 pav.:

¹³ The National Election Committee. (2005) E-voting system overview [interaktyvus]. Talinas: The National Election Committee

¹⁴ EPP, M. (2007) Internet voting system [interaktyvus]. Talinas: Estonian National Electoral Committee.



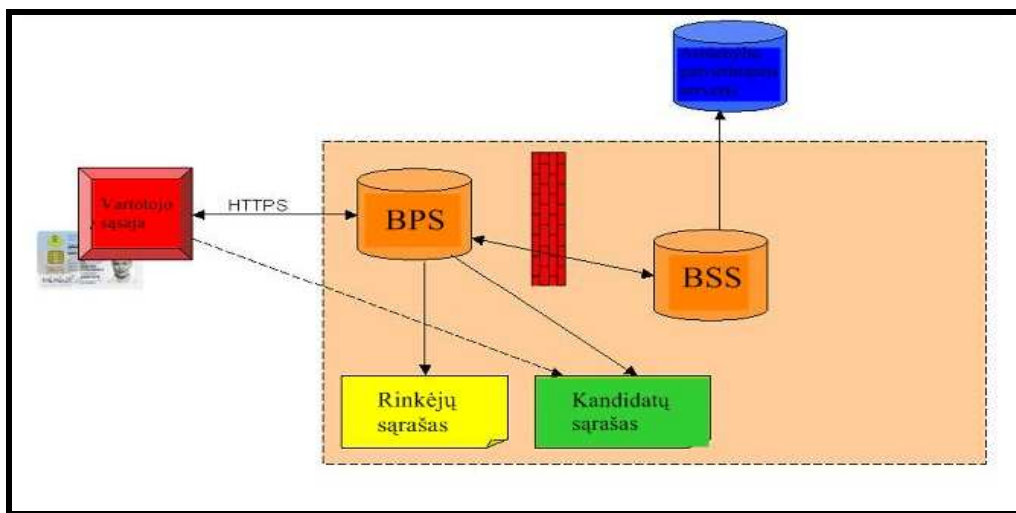
Šaltinis: THE NATIONAL ELECTION COMMITTEE. (2005) E-voting system overview, p. 9.

3 pav. Estijos elektroninio balsavimo sistemos projekto architektūra.

Rinkėjas sukuria užšifruotą ir skaitmeniniu parašu pasirašytą balsą ir siunčia jį į centrinę sistemą. **Centrinė sistema** priima ir apdoroja balsus kol suminiai el. balsavimo rezultatai yra išduodami. **Rakto vadyba** generuoja ir valdo sistemos raktų poras. Viešasis raktas yra integruotas į rinkėjo aplikaciją, privatus raktas yra pristatomas į balsų skaičiavimo serverį. Estijos el. balsavimo sistema atkreipia svarbų dėmesį į sistemos auditą. **Auditas** sprendžia konfliktus ir nusiskundimus, naudodamas log failuose išsaugotą informaciją iš centrinės sistemos¹⁵. Šis faktorius kaip vienas iš būtinų yra įvardintas P.G. Neumann (1993), jis aprašo, kad visos operacijos turi būti stebimos, bet vartotojo konfidencialumas nepažeidžiamas. Taip pat vykdomas auditas turi vykti visą balsavimo laikotarpį. Turi būti stebima kiek balsų buvo užregistruota ir suskaičiuota galutiniame rezultate (Neumann, P.G., (1993)). **Vartotojo sąsaja** - internetinė aplikacija. Šifravimas ir autentifikacija sukurti SSL protokolo pagrindu, apsaugo komunikaciją tarp rinkėjo ir balsus perduodančio serverio. Estijos el. balsavimo sistema gali veikti Windows, Linux ir MacOS operacinėse sistemose. Viešasis raktas yra integruotas į balsavimo aplikaciją. Balsuojančio asmens aplikacija naudoja ActiveX aplikaciją. Centrinė sistema yra padalinta į dvi dalis: balsuojančių asmenų sąrašų kompiliatorių (Populiacijos registrą) ir kandidatų sąrašų kompiliatorių. **Balsus perduodantis serveris (BPS)** – autentifikuoja rinkėją ID kortelės pagalba, parodo kadidatus iš jo rinkimų apygardos ir priima užšifruotą ir skaitmeniniu parašu patvirtintą el. balsą. **Balsus saugantis serveris (BSS)** – priima el. balsus iš BPS ir juos saugo. Po el. balsavimo pabaigos išima besidubliuojančius balsus, atšaukia balsus asmenų, kurie neturėjo teisės balsuoti ir priima bei

¹⁵ The National Election Committee. (2005) E-voting system overview [interaktyvus]. Talinas: The National Election Committee.

apdoroja el. balsų atšaukimus. Po to atskiria vidinius vokus nuo išorinių vokų ir paruošia juos Balsus skaičiuojančiam serveriui. **Balsus skaičiuojantis serveris (BSA)** – ne tinkle veikiantis komponentas, prie kurio prieiti iš išorės negalima, į kuri užšifruoti balsai yra perkeliami su „nuimtu“ skaitmeniniu parašu. BSA naudoja privatų sistemos raktą, sudaro iš balsų lenteles ir išduoda el. balsavimo rezultatus. **Teisėtumą patvirtinantis serveris (TPS)** – ne Centrinės sistemos dalis, jis reikalingas ID kortelių teisėtumui patvirtinti, be kurių skaitmeninis parašas negalioja¹⁶.



Saltinis: THE NATIONAL ELECTION COMMITTEE. (2005) E-voting system overview, p. 12.

4 pav. Estijos el. balsavimo sistemos balsavimo proceso komponentai.

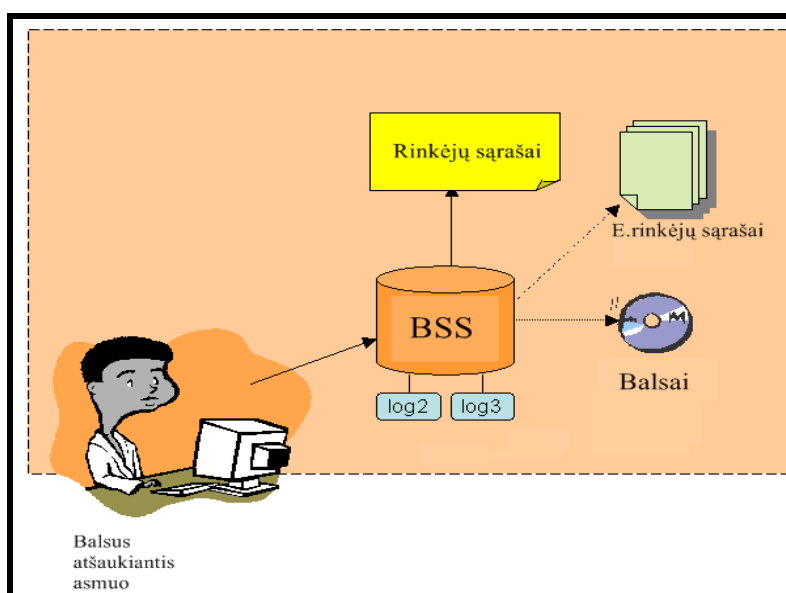
Balsavimo procesas vyksta:

1. Rinkėjas per HTTPS protokolą pasiekia BPS ir identifikuoja save su ID kortele.
2. BPS suformuoja užklausą naudodamas rinkėjo asmeninį identifikacijos kodą (AIK) iš rinkėjų DB, patikrina jo galimumą balsuoti ir nustato jo ar jos rinkimų apygardą. Jei rinkėjas negali balsuoti, jam pristatoma žinutė ir jis nukreipiamas į X-tee paslaugą, teikiamą Populiacijos registro, kur jis ar ji gali patikrinti savo teisę balsuoti.
3. BPS formuoja užklausą iš BSS tam, kad išsiaiškinti ar šis rinkėjas jau balsavo. Jei jis jau balsavo, apie tai yra informuojamas.
4. BPS sudaro užklausą naudodamas rinkimų apygardos informaciją iš kandidatų sąrašų DB ir gauna rezultatą: kandidatų sąrašą toje rinkimų apygardoje. Šis sąrašas atvaizduojamas rinkėjui;
5. Rinkėjas išsirenka kandidatą;
6. Vartotojo sąsaja, turinti kandidatų sąrašą, pareikalauja, vartotojo patvirtinti jo pasirinkimą;
7. Ši sąsaja užšifruoja pasirinkimą ir atsitiktinai sugeneruotas skaičius su BSA viešuoju raktu. Rinkėjas pasirašo kriptogramą su jo skaitmeniniu parašu.

¹⁶ The National Election Committee. (2005) E-voting system overview [interaktyvus]. Talinas: The National Election Committee.

8. Vartotojo sąsaja persiunčia skaitmeniniu parašu pasirašytą kriptogramą į BPS, kuris patikrina formalų teisingumą gautos medžiagos ir ar tas pats žmogus, kuris autentifikavosi sesijos pradžioje padėjo SP.
9. BPS siunčia toliau priimtą balsą į BSS. BSS pasiekia teisėtumą tvirtinantį serverį (TTS) ir pasiima sertifikatą, patvirtinantį SP teisėtumą.
10. Sėkmingo balsavimo atveju BSS siunčia patirtinimą BPS, kad balsas buvo priimtas. Atitinkama žinutė taip pat pasiekia rinkėją.
11. Balsuojantis asmuo gali balsuoti keletą kartų. Visi balsai yra perduodami per BPS į BSS.
12. Po el. balsavimo pabaigos BPS atsijungia nuo visų komunikacijų. TTS yra nepasiekiamas balsavimo metu, balso priėmimo laikas yra išsaugomas ir teisėtumą patvirtinantis servisas leidžia patikrinti sertifikato teisėtumą vėlesniuose etapuose. Laikas sistemos ir teisėtumą patvirtinančiame serveryje turi būti sinchronizuotas¹⁷.

BSS yra centrinis komponentas balsų atšaukimui ir saugojimui. Proceso rezultatas yra balsai – užšifruoti kandidatų numeriai, nuo kurių nuimti skaitmeniniai parašai ir sąrašai rinkėjų, kurie balsavo el. balsavimo metu. 5 pav. atvaizduotas balsų rūšiavimas ir atšaukimas.



Šaltinis: THE NATIONAL ELECTION COMMITTEE. (2005) E-voting system overview, p. 14.

5 pav. Balsų rūšiavimas ir atšaukimas Estijos el. balsavimo sistemoje

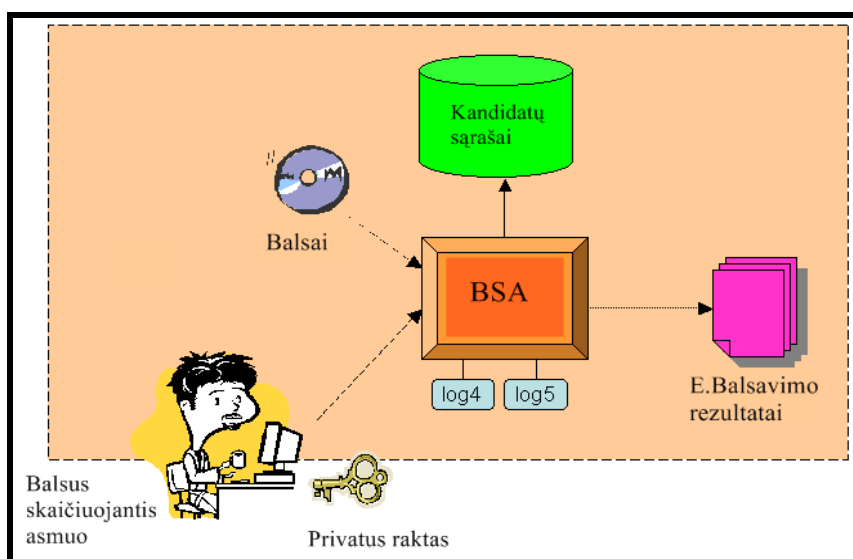
1. Iš karto po išankstinio balsavimo pabaigos dvigubi balsai yra atšaukiami. Tik paskutinis balsas yra įskaitomas. Kiekvienas atšauktas balsas yra įrašomas į log LOG2. Galimos priežastys: daugkartinis balsas, dalyvavimas išankstiniuose rinkimuose, balsavimas rinkimų dieną. Po

¹⁷ The National Election Committee. (2005) E-voting system overview [interaktyvus]. Talinas: The National Election Committee.

dvigubų balsų atšaukimo el. rinkėjų sąrašai (vardas, ID, numeris balsavimo sąrašė) yra sukompilijuojami ir siunčiami į balsavimo stotis tuo pačiu metu kaip ir išankstinių rinkimų vokai.

2. Balsų atšaukimo etapas, kuris baigiasi rinkimų dieną 20.00 val. Pirmiausia žmonės, kurie balsavo el. rinkimuose, rinkimuose paštu.
3. Rinkimų dieną iš sąrašo rinkėjų balsavusių rinkimų dieną įprastu balsavimo būdu, NRK sudaro bendrą sąrašą, ir perduoda BSA.

Balsų skaičiavimas vyksta BSA, atskirtame nuo tinklo. Taip pat turi būti prieinami kandidatų sąrašai. Reikalaujama, kad būtų realizuotas balsų perskaičiavimas. Sistemos privatus raktas yra aktyvuojamas rakto vadybininkų. Balsavimo skaičiavimo įeinantys duomenys yra balsai paimti iš BSS išorinėje laikmenoje ir surūšiuotoje pagal balsavimo apygardas. El. balsavimo rezultatai yra pridedami prie rezultatų gautų balsuojant balsavimo dėžėse¹⁸.



Šaltinis: THE NATIONAL ELECTION COMMITTEE. (2005) E-voting system overview, p. 16.

6 pav. Balsų skaičiavimas Estijos el. balsavimo sistemoje

1.3.4 Šveicarijos elektroninio balsavimo sistema

Šveicarijoje elektroninio balsavimo eksperimentai buvo įvykdyti trijuose kantonuose 2003 m., taip pat penki bandomieji balsavimai įvykdyti 2004 ir 2005 m. nacionaliniuose referendumuose

¹⁸ The National Election Committee. (2005) E-voting system overview [interaktyvus]. Talinas: The National Election Committee.

Ženevos, Niurnbergo ir Ciuricho kantonuose¹⁹. Be išlygų, visi penki bandymai atlikti sėkmingai ir be jokių nenumatytų atsitikimų (Krimmer, R. (2006)).

2 lentelė

Bandomieji balsavimai Šveicarijoje

Data	Kantonas	Rinkėjų skaičius	El. balsų skaičius (dalis % nuo visų gautų balsų)
2004-09-26	Ženeva	22 137	2 723 (21,8 %)
2004-11-28	Ženeva	41 431	3 755 (22,4 %)
2005-09-25	Niurnbergas	1 732	1 178 (68,0 %)
2005-11-27	Ciurichas	16 762	1 154 (22,1 %) (243 SMS žinute)
2005-11-27	Niurnbergas	2 469	1 345 (55,1 %)

Šaltinis: KRIMMER, R. (2006) D. Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed, p. 30.

Kaip matoma iš lentelės 5 bandomieji balsavimai buvo sėkmingi ne tik tuo, kad juose nebuvo jokių nenumatytų atsitikimų, bet ir tuo, kad procentaliai iš visų galinčių balsuoti rinkėjų elektroninio balsavimo būdu balsavo nuo 21,8% iki net 68% rinkėjų. Šveicarijos el. balsavimo sistemos privalumai: išaugęs dalyvaujančių rinkimuose piliečių skaičius. Pagrindinės priežastys: jauni žmonės dėl interneto vartojimo masto, pagyvenę asmenys dėl su mobilumu susijusių problemų, piliečiai gyvenantys užsienyje dėl sudėtingos pašto veiklos, akli arba silpnaregiai rinkėjai (Krimmer, R. (2006)). Balsavimo etapai:

1. Tam, kad rinkėjas būtų priimtas į balsavimo serverį, rinkėjas privalo įvesti teisingą balsavimo 16 skaitmenų kortelės numerį. Po šio žingsnio rinkėjas gauna informaciją apie baudas apgavystės atveju bei el. balsavimo biuletenį ekrane.
2. Rinkėjas balsuoja pažymėdamas „Taip“ arba „Ne“ prie kiekvieno klausimo. Arba palikdamas nepažymėtą atsakymą, tuomet tai traktuojama kaip susilaikymas tuo klausimu.
3. Sistema reikalauja rinkėjo patvirtinti savo pasirinkimą. Kontrolinis kodas yra naudojamas patikrinti ar rinkėjas balsavo efektyviai. Rinkėjas yra klausiamas identifikuoti save: gimimo datą, gimimo vietą ir ID ant balsavimo kortelės, padengtos nutrinamu sluoksniu. Sistema patvirtina, jog balsas priimtas, parodydama registracijos laiką ir datą²⁰.

Rezultatų skaičiavimas reikalauja kontrolierių dalyvavimo, kurie įveda savo privačius raktus į sistemą. Jie taip pat turi slaptažodžius, kurie leidžia registruotus balsus užšifruoti dvigubai.

¹⁹ Federal Office of Communications OFCOM. (2007) [Electronic voting](#) [interaktyvus]. Šveicarijos konfederacija: Federal Office of Communications.

²⁰ State Chancellery. (2007) State Council's Report to the Grand Council on the Geneva electronic voting project [interaktyvus]. Republic and Canton of Geneva: State Chancellery.

Sistema generuoja du failus: vienas failas biuletenių, turintis vaizdą kiekvieno biuletenio registruoto per balsavimo puslapį. Kitas failas paimtas iš rinkimų sąrašo, leidžiantis atlikti statistinę balsavusių rinkėjų analizę. Jis susideda iš rinkėjų duomenų. Po rinkimų rezultatai saugomi 50 dienų, po to CD ir biuleteniai yra sunaikinami (Krimmer, R., (2006)). 6 lentelėje palyginama Šveicarijos el. balsavimo sistema su balsavimu paštu.

3 lentelė

Šveicarijos el. balsavimo sistemos ir balsavimo paštu palyginimas

El. balsavimui keliami reikalavimai	Analogiškumas su balsavimo paštu metodu	Priemonės, naudotos rinkimų metu el. balsavimo sistemoje
Rinkėjo autentifikacija: Rinkėjas, dalyvaujantis rinkimuose identifikuojamas kaip asmuo, kuris jis skelbiasi esąs.	Galintys balsuoti rinkėjai, pasirašo ranka ant balsavimo leidimo ar ant voko. Balsavimo lapeliai užpildomi ranka.	<ul style="list-style-type: none"> • Individualus ir saugus prieigos kodas; • Patvirtinimas įvedant gimimo datą ir/ar gimimo vietą; • Skaitmeninio parašo panaudojimas (ateityje).
Sistemos autentiškumas: Rinkėjai privalo žinoti, jog Jų balsai pakliūs į reikiamą balsavimo dėžę ir galutinio skaičiavimo metu bus įskaičiuoti į galutinį rezultatą.	Paštu balsai yra pristatomi pašto tarnybos, perduodami pašto tarnautojo arba siunčiami per bendruomenės pašto dėžutę.	<ul style="list-style-type: none"> • SSL gali būti patikrintas rinkėjo naudojant jo piršto antspaudą. • Serverio autentiškumas gali būti atliktas patikrintant atsakantį kodą ar/ir vaizdinius simbolius.
Vienintelis balsas: Rinkėjo balsas gali būti įskaičiuotas į galutinį balsų skaičiavimą tik vieną kartą.	Balsavimo lapelis išleidžiamas tik kartą. Užpildytas lapelis siunčiamas atgal voke. Pakartotinis balsavimas neįmanomas.	<ul style="list-style-type: none"> • Įgaliojimų nutraukimas, priėjimui prie balso, kai tik jis registruojamas balsavimo dėžėje; • Aiškūs ženklai ant balsavimo voko (nenulaužiamas antspaudas per slaptą priėjimo kodą), parodantis, kad rinkėjas jau balsavo elektroniniu būdu.

3 lentelės tęsinys

El. balsavimui keliami reikalavimai	Analogiškumas su balsavimu paštu	Priemonės, naudotos rinkimų metu el. balsavimo sistemoje
<p>Balsavimo slaptumo/duomenų apsauga: Rinkėjo pasirinkimas turi išlikti slaptas.</p>	<p>Balsavimo lapeliai municipalinį ofisą pasiekia atskirai antspauduotame voke. Po parašų patvirtinimo, balsavimo leidimai ir balsavimo lapeliai turi būti atskirti.</p>	<ul style="list-style-type: none"> • Atskirai saugoma asmeninė informacija ir rinkėjo balsai. • Nuolatinis balsų maišymas elektroninėje balsavimo sistemoje, siekiant atsitiktinio generatoriaus.
<p>Pasiruošimas apsaugojimui nuo stichinių nelaimių ir kitų nenumatytų įvykių: audrų, elektros tiekimo nutraukimui.</p>	<p>Analogiškos grėsmės egzistuoja ir balsuojant paštu, balsavimo patalpoms, balsavimo lapelius pristatančioms tarnyboms, balsų rūšiavimo ofisams.</p>	<ul style="list-style-type: none"> • Keleto atsarginių serverių naudojimas; • Serverių apsauga: laikymas saugiose patalpose (įėjimo kontrolė, apsauga, atsarginis elektros tiekimas).
<p>Atkuriamumas ir įrodomumas: Turi būti realizuotas balsų perskaičiavimas, esant labai artimiems rinkimų rezultatams ar skundo atveju.</p>	<p>Popieriniai balsavimo biuleteniai gali būti bet kada perskaičiuoti, netgi dalyvaujant stebėtojams.</p>	<ul style="list-style-type: none"> • Paruošimas standartinių ir elektroninių įrašų, kurie yra pasirašyti tiesioginės už tai atsakingos valdžios; • Paruošimas išorinės laikmenos (balsavimo rezultatų ir log failų duomenys); • Iš partijų atrinktų stebėtojų dalyvavimas.
<p>Patikimumas: Visa balsavimo procedūra privalo būti patikima ir prireikus patikrinama.</p>	<p>Balsavimas paštu yra užsitarnavęs didelį pasitikėjimą.</p>	<ul style="list-style-type: none"> • Inspektorių įtraukimas visuose procesuose; • Nepriklausomas kodo tikrinimas, atviro kodo metodas; • Paskelbimas privačių aplikacijų.
<p>Apsauga nuo išorinių atakų: a) Galutinio vartotojo įrenginiai (asmeniniai kompiuteriai, mobilūs telefonai) galimas balsų perėmimas ir pakeitimas.</p>	<p>Balsai yra pavogiami po balsavimo. Sisteminis piktnaudžiavimas negali būti išskirtas, jei balsavo nedaug rinkėjų ir jie nepažymėjo savo pasirinkimo balsavimo biuletenyje.</p>	<ul style="list-style-type: none"> • Sudėtinė apsauga ugniasienių pagalba; • Balsavimo kodo metodai (Ciuricho SMS, balso perdavimas ryšio kanalu kaip skaičių seka); • Antivirusinių programų panaudojimas.

3 lentelės tęsinys

El. balsavimui keliami reikalavimai	Analogiškumas su balsavimu paštu	Priemonės, naudotos rinkimų metu el. balsavimo sistemoje
<p>b) Balso perdavimas nuo vartotojo sąsajos iki BPS: Galimas įsiterpimas ir balsų pakeitimas.</p>	Balsai gali pakliūti į blogas rankas ar būti sunakinti, jei jie išimami iš bendruomenės pašto dėžutės ar balsų maišelis pavogiamas transportavimo metu.	<ul style="list-style-type: none"> • Balso šifravimas (SSL); • Balso detalės perduodamos grafiškai ne kaip tekstas; • Visi gaunami paketai testuojami dėl jų vientisumo, naudojant horizontalias kontrolines sumas.
<p>c) Platforma: apsauga nuo atakų.</p>	Balsadėžės tyčinė ataka arba balsų perdavimas yra nutrauktas dėl pašto tarnybos gedimų	<ul style="list-style-type: none"> • Panaudojimas keleto atsarginių serverių; • Bendradarbiavimas su keletu tiekėjų.

Šaltinis: Krimmer R. (2006) Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed, p. 8-9.

1.3.5 Europos tarybos ministrų komiteto požiūris į el. balsavimą

Europos tarybos ministrų komitetas patikėjo daugiadisciplininei teisinės, sistemos veikimo bei techninių sričių specialistų grupei užduotį sukurti standartų rinkinį, kurie būtų naudojami šalių narių, kuriant el. balsavimo sistemas. Ši darbo grupė išleido rekomendaciją, kuri apima daugiau nei 100 standartų bei principų. Pagrindiniai reikalavimai el. balsavimo sistemai: skaidrumas, atviri standartai, sistemos auditas, sertifikavimas, informacijos suteikimas, apmokymai bei pagalba. Teisiniai standartai: el. balsavimas negali būti privalomas, rinkėjas turi turėti teisę pakeisti savo pasirinkimą kiekvienam el. balsavimo taške, prieš užregistruojant balsą, sistema turi neleisti pakeisti balsą, kai jis jau užregistruotas. El. balsavimo sistema privalo leisti rinkėjui užregistruoti tuščią balsą. Šalys narės turi užtikrinti, kad rinkėjai supranta ir pasitiki el. balsavimo sistema. Informacija apie jos funkcionavimą turi būti visuotiniai prieinama. Rinkėjams turi būti suteikta galimybė išbandyti bet kurį naują el. balsavimo metodą prieš balsuojant elektroniniu būdu. Patikrinimo bei sertifikavimo tikslai reikalauja, kad el. balsavimo sistemos komponentai turi būti atviri, bent jau kompetetingoms rinkėjų institucijoms. El. balsavimo sistema privalo užtikrinti galimybę perskaičiuoti balsus. Veikimo standartai: pagalbos bei nuorodų išdėstymas balsavimo procedūrose turi būti prieinamas rinkėjams, naudojant bet kurį el. balsavimo kanalą. El. balsavimo sistema turi neleisti rinkėjui suabejoti, ar jo balsas užregistruotas ar ne. El. balsavimo sistema privalo neatskleisti užregistruotų balsų skaičiaus iki rinkimų pabaigos. Skaičiuojant balsus, kompetetingi rinkimų institucijų atstovai privalo sugebėti dalyvauti balsų skaičiavime. El. balsavimo

sistema turi būti audituojama. Technologiniai reikalavimai: vartotojai turi būti įtraukti į el. balsavimo sistemos kūrimą, ypač identifikuojant suvaržymus ir testuojant naudojimosi ja patogumą kiekvienam sistemos vystymo etape. Prieinamumas - aklieji vartotojai turi aprūpinti papildomais įrenginiais, tokiais kaip specialios sąsajos ar kiti panašūs resursai, tokie kaip asmeninė pagalba. Atviri standartai turi būti naudojami užtikrinti, kad skirtingi el. balsavimo sistemos technologiniai komponentai ar paslaugos, pristatomos iš skirtingų šaltinių, veikia kartu. Audito sistema, leidžianti visapusišką auditą turi būti sukurta bei įdiegta kaip dalis el. balsavimo sistemos. Certifikavimo procesas, leidžiantis ištestuoti ir certifikuoti bet kurį ICT komponentą bei suderintas su atitinkamais technologiniais reikalavimais turi būti įdiegtas²¹.

²¹ eGovernment News. (2004) EU: E-voting systems must be based on open standards, says Council of Europe [interaktyvus]. European Communities 2004.

El. balsavimo sistemos saugumo aspektai

El. balsavimo sistemos problemos		Technologinės grėsmės	Galimos atsakomosios priemonės saugumui užtikrinti
1.	Apsimetimas dėl teisės balsuoti, kuomet asmuo bando apsimesti teisėtu rinkėju, neturėdamas tam teisių: registracijos procese turi būti tikrinama ir patvirtinama, kad asmuo turi teisę balsuoti.	Netinkama, neteisinga asmens autentifikacija rinkėjų registracijos metu.	Patikima kandidato autentifikacija ir registracija yra reikalinga naudojant: saugumo procedūras, geriausių pavyzdžius, saugius ryšio kanalus, kandidatų autentifikaciją, rinkėjų registracijos institucija privalo laikytis saugumo operacijų procedūros standarto.
	Teisė balsuoti turi būti suteikta tik po tinkamo patikrinimo, užtikrinančio, kad asmuo turi balsavimo teisę.	Netinkamas privatumo užtikrinimas tarp asmens ir rinkimų sistemos per rinkėjų registraciją.	Kanalas tarp rinkėjo ir registravimo sistemos turi užtikrinti: ryšį, konfidencialumą bei ryšio vientisumą.
2	Dėl neteisingo kandidato identifikavimo rinkėjas nėra supažindintas su teisinga balsavimo informacija.	Neteisinga identifikacija kandidatų registracijos metu.	Patikima kandidato autentifikacija ir registracija yra reikalinga naudojant: saugumo procedūras, geriausių pavyzdžius, saugius ryšio kanalus, kandidatų autentifikaciją, rinkėjų registracijos institucija privalo laikytis saugumo operacijų procedūros standarto.
3	Registravimo sistemos nuasmeninimas.	Netinkama registravimo sistemos autentifikacija.	Kanalai iš ir į registracijos sistemą turi teikti "point to point" autentifikaciją.
4	Apsimetimas teisėtu registruotu rinkėju.	Neteisinga rinkėjo autentifikacija, atliekant balsavimą.	Patikima rinkėjo autentifikacija (t. y. teisė balsuoti).
		Netinkami mainai tarp rinkėjo ir rinkimų sistemos, kai balsas yra registruojamas.	Kanalas turi teikti ryšio konfidencialumą bei vientisumą.
5.	Neteisėtas balsavimo teisės pasisavinimas iš teisėto rinkėjo. Tai gali būti atlikta bauginimo, vagystės ar bet kokių kitu būdu, kai balsavimo teisės gaunamos nelegaliai.	Rinkėjo balsavimo kortelės vagystė. Įvairūs būdai gauti teisėto rinkėjo duomenis.	Tam tikra slapta informacija, žinoma tik rinkėjui yra reikalinga atliekant balsavimą. Prieš įskaičiuojant balsą, kaip validų, įrodymas turi būti pateiktas, kad rinkėjo slapta informacija buvo pristatyta, balso užregistravimo metu.

4 lentelės tęsinys

Eil. Nr.	El. balsavimo sistemos problemos	Technologinės grėsmės	Galimos atsakomosios priemonės saugumui užtikrinti
6.	Balsavimo sistemos nuasmeninimas.	Netinkama registravimo sistemos autentifikacija. Netinkama balsaežės autentifikacija.	Kanalas turi užtikrinti "point to point" autentifikaciją.
7.	Rinkėjas nėra supažindintas su teisinga balsavimo informacija.	Netinkamas balsavimo informacijos vientisumas suteiktas rinkėjui ar sukurtas balsavimo sistemoje. Balsavimo parinktys pateiktos rinkėjui yra netikros. Trojan'ai, "man in the middle attack".	Patikimas kelias į rinkėją balsavimo informacijos vientisumas. Užregistruotų balsų vientisumas. Patikimas kelias tarp rinkėjo ir balso įrašymo. Patikimas kelias į rinkėją balsavimo parinktyse.
8.	Suvokimas, kad el. balsavimo sistema įrašo balsus tinkamai.	Balsavimo sistemos vientisumas. Nesaugus kanalas tarp rinkėjo ir balsus registruojančio taško. Rinkėjo sprendimas yra įrašomas tiksliai. Įrodymas, kad tikrasis balsas buvo tiksliai įskaičiuotas į rezultatus.	Balso neatsisakymas, kurį atliko tikrasis rinkėjas, balsavimo sistemos auditas bei ryšio konfidencialumas. Ryšio vientisumas. Ryšio konfidencialumas. Patikimas kelias tarp rinkėjo ir balso įrašymo. Neatsisakymas įrašyto balso. Auditas.
9.	Užtikrinimas, kad rinkėjo slapta pasirenkimas bus neatskleistas.	Rinkėjo asmenybė yra atskleista.	Rinkėjo asmenybė yra anonimiška Balsas išlieka konfidencialus.
10.	Užtikrinimas, kad rinkėjo balsas buvo užregistruotas.	Balso praradimas.	Balso pridavimo įrodymas.
11	Kaip rinkėjas gali būti tikras, kad "man-in-the-middle" ataka nebus atlikta, balsui pakeisti.	Pažeidžiama kliento aplinka, "Trojan'ai" bei virusai. Ryšio perėmimas.	Fizinė apsauga. Procedūrinė apsauga. Nepažeidžiama, užkoduota balsavimo informacija. Ryšio kanalo vientisumas tarp kliento ir serverio sistemos.

4 lentelės tęsinys

Eil. Nr.	El. balsavimo sistemos problemos	Technologinės grėsmės	Galimos atsakomosios priemonės saugumui užtikrinti
12.	Visi skaičiuojami balsai turi būti atlikti teisėtų rinkėjų.	Rinkėjo nuasmeninimas, audito įrankiai nepajėgūs pateikti tinkamus įrodymus.	Rinkėjo autentifikacija. Neatsisakymas balso įrašo. Neatsisakymas, kad teisėti rinkėjai atliko visus balsus. Nepriklausomas auditas.
13.	Vienas balsas iš vieno rinkėjo per vienus rinkimus.	Rinkėjas nuasmeninimas registracijos metu. Kelios registracijos paraiškos. Skirtingi rinkėjų įgaliojimų pasiskirstymai.	Vartotojo registracijos apsauga, procedūros ir rinkėjo identifikacija. Rinkėjo autentifikacija.
14.	Balsas negali būti pakeistas rinkėjo ketinimu.	Pažeidžiama kliento aplinka, "Trojan'ai" bei virusai.	Patikimas kelias nuo rinkėjo ketinimo iki balso įrašymo, balso vientisumas ir balso neatsisakymas.
15.	Balsai negali būti atskleisti prieš rinkimų pabaigą.	Balsai gali būti atskleisti prieš rinkimų pabaigą.	Rinkėjo konfidencialumas.
16.	Balsavimo sistema turi būti atskaitinga ir tikrintina.		Neatsisakymas balso duomenų ir audito įrankiai.
17.	Informacijos iš ir į rinkėją identifikacija ir autentiškumas turi būti apsaugotas, laikantis privatumo nuostatų.	Privatumo praradimas.	Kanalas turi užtikrinti ryšio konfidencialumą.
18.	Rinkėjo tikroji asmenybė turi būti anonimiška.	Rinkėjo asmenybė yra atskleista.	Rinkėjo identifikacija yra anonimiška.
19.	Uždraustas priėjimas prie el. balsavimo serverio.		Sistema turi būti sukurta taip, kad būtų atspari išorinėms atakoms ir turėtų atsarginį planą atakos atveju.

Šaltinis: BORRAS, J. (2007) Election Markup Language (EML) Version 5.0, p. 39-43.

1.4 Pasitikėjimo el. balsavimo sistemomis veiksmų analizė

Apžvelgus elektroninių balsavimo sistemų modelius bei projektus, bei apibendrinus pasitikėjimo el. valdžia teorinius modelius, tolimesnis žingsnis yra atlikti el. balsavimo sistemose egzistuojančių pasitikėjimą kuriančių veiksmų analizę.

5 lentelė

Pasitikėjimui Lietuvos el. balsavimo sistema kylančios grėsmės

Problema	Keliamos grėsmės
Sistemos skaidrumas	Sudėtingomis technologijomis paremta sistema niekada nebus skaidri didžiajai daugumai LR piliečių.
Sistemos saugumas	Vartotojo kompiuterio saugumo (virusai), VRK serverio sertifikavimo problema.
Rinkimų slaptumas	Rinkėjui balsavus, jo balsas gali būti atskleistas. Tai neturėtų įtakos rinkimų rezultatams, tačiau pati sistema tampa nepatraukli rinkėjams.
Rinkimų tikslumas	Neatliekant balsų skaičiavimo serverio sistemos audito, įmanoma manipuliuoti ne pačiais balsais, o pakeisti skaičiavimo algoritmus taip, kad būtų gaunamas „reikalingas“ rezultatas.
El. bankininkystės sistemos panaudojimas el. balsavimui.	Sunku užtikrinti, kad su rinkimais susijusi informacija bus visiškai neprieinama bankams, kurie yra privatūs subjektai ir kurių veiklą valstybė gali kontroliuoti tik įstatymais numatytuose rėmuose.
Visuomenės pasitikėjimo valdžios institucijomis, rinkimais, partine sistema.	Bendras Lietuvos visuomenės pasitikėjimo valdžios institucijomis lygis, visuomenės pasitikėjimas rinkimų teisėtumu, Lietuvos partinės sistemos konfliktiškumo laipsnis, vertinant tikimybę, jog tam tikros politinės jėgos galėtų sąmoningai siekti sukelti pasitikėjimo krizę. Kaip rodo 2007 m. atliktas Lietuvos gyventojų vertybių tyrimas, Lietuvos žmonės ne tik nepasitiki valdžios institucijomis, bet nėra patenkinti ir pačia politine santvarka.

Šaltinis: sudaryta autoriaus pagal RAMONAITĖ, A. (2008) Elektroninio balsavimo galimybių studija; DAMBAUSKAS E. (2007) Analitinė studija: Dėl LR Seimo nutarimo „Dėl balsavimo internetu rinkimuose ir referendumuose koncepcijos patvirtinimo”.

6 lentelė

Pasitikėjimui Estijos el. balsavimo sistema kylančios grėsmės

Problema	Keliamos grėsmės
Rakto vadyba	Privatumas ir slaptumas el. rinkėjo gali būti sukompromituotas, jei vienu metu vyksta du pavojai: atsiranda suinteresuota šalis sistemoje (ar už sistemos ribų), kuri turi priėjimą prie abiejų privataus rakto bei prie skaitmeniniu parašu patvirtintų balsų. Nors ši informacija atskirta nuo sistemos, tačiau rizika išlieka. Visgi privatų raktą apsaugoti lengviau neskaitmeniniu parašu patvirtintus balsus, kurie pereina per VS, BPS, BSS ir duomenų perdavimo kanalus, be to pavojus dėl nutekėjusių balsų yra didesnis.
Rinkėjų privatumas	Paviešinimo grėsmė. Šių grėsmių pasirodymas įgalintų kartu su skaitmeniniu parašu patvirtintais balsais nustatyti, kas balsavo, taip pažeidžiant rinkėjo privatumą.
Rakto saugumas	Privatus raktas gali būti sunaikintas, pamestas ar iškraipytas dėl techninių priežasčių. Tai lemtų, kad el. balsai būtų neiššifruojami ir būtų prarasti.

Šaltinis: sudaryta autoriaus

Pasitikėjimui Šveicarijos el. balsavimo sistema kylančios grėsmės

Problema	Keliamos grėsmės
Balsų konfidencialumas	Rinkėjai gali atiduoti konfidencialią savo informaciją netikram internetiniam puslapiui, to net neįsivaizduodami. Panaudodamas pavogtą informaciją atakos vykdytojas galėtų balsuoti savo nuožiūra.
Balsų saugumas	Komunikavimo kanalas tarp rinkėjo ir serverio gali būti nepakankamai saugus.
Pakartotinis balsavimas	Rinkėjui pakeitus apsisprendimą po balsavimo. Balso keisti nebegalima.

Šaltinis: sudaryta autoriaus

1.5 Teorinio skyriaus išvados

Buvo išanalizuoti teoriniai pasitikėjimo el. valdžia modeliai. Jie gali būti suskirstyti į dvi grupes: veikiančius prieš sąveiką su sistema ir sąveikos metu. Apibendrintas pasitikėjimo el. valdžia teorinis modelis susideda iš piliečio, el. valdžios sistemos ir technologijų bei trečiosios šalies. Prieš sąveiką veikiantys veiksniai tai - individualaus piliečio elgesio požymiai, instituciniai bei technologiniai veiksniai. Sąveikos metu veikia paslaugos, tranzakcijos išpildymo bei informacijos atributai. Individualaus piliečio elgesio požymiai tai subjektyvios jo normos, individuali demografija, bendros intencijos pasitikėjimui ir el. paslaugų naudojimas, kitų asmenų nuomonė bei patirtis, kultūra bei tradicijos. Instituciniai veiksniai šiuo atveju tai - valdžios institucija, kurios reputacija, patikimumas, įstatyminiai reikalavimai bei kompetencija veikia rinkėjo pasitikėjimą. Technologiniai faktoriai lengviausiai paveikiami iš sistemos kūrėjų pusės, bei aktyviausiai vartotojui. Svarbiausi šios grupės aspektai yra perdavimo kokybė sąsajos dizainas ir sudėtis, saugumas, skaitmeninis sertifikatas, viešojo rakto infrastruktūra, vientisumas, kompetencija ir nuspėjamumas, privatumas, tranzakcijos nuoseklumas, prieinamumas ir konfidencialumas. Sąveikos su sistema metu veikiantys paslaugos požymiai patikimumas, pritaikomumas individualiam vartotojui, prieinamumas ir kokybė: informacija, vartotojo sąsajos draugiškumas ir estetika yra ne mažiau svarbūs el. valdžios paslaugų vartotojui. Be to tranzakcija turi išpildyti šiuos reikalavimus: skaidrumas, aptarnavimas po tranzakcijos įvykdymo, tikslumas ir kokybė. Paskutinioji veiksmų grupė siekia užtikrinti pasitikėjimą informacijos savybėmis, nustatydamas, kad ji turi būti tiksli, išbaigta, nešališka, patikima, aplinka, naudinga ir kokybiška.

Išanalizavus sistemas pagrindiniai skirtumai tarp jų yra tai, kad Estijos el. balsavimo sistema naudoja ID korteles su skaitmeniniu parašu, o Šveicarijos realizuota el. balsavimo sistemoje panaudota balsavimo kortelės su nutrinamu sluoksniu. Autentifikacija vykdoma jau minėtų kortelių pagalba, tačiau įvedant skirtingus kodus, be to Estijos el. balsavimo sistema pasižymi galimybe

balsuoti pakartotinai. Balsavimas bei balsų saugojimas panašūs tuo, kad šiose fazėse siekiama išsaugoti rinkėjo privatumą bei rinkimų saugumą. Be to Šveicarijos el. balsavimo sistemoje realizuotas puslapis, kuriame vartotojas gali pasitikrinti ar jo balsas pateko į galutinę balsadėžę. Balsų valdyje svarbus yra balsų perdavimas – Estijos el. balsavimo sistemoje naudojamas dvigubas šifravimas, o Šveicarijos sistemoje šifravimas bei balso konvertavimas į grafinį vaizdą. Rinkėjams svarbus aspektas, kad abi sistemos siekia išsaugoti rinkėjo privatumą ir prieš balsų skaičiavimo fazę atskiria rinkėjų sąrašus nuo jų balsų. Balsų skaičiavimas vykdomas nuo tinklo atskirtame serveryje, bei balsavimo rezultatai saugomi atitininkamą laikotarpį abiejose nagrinėtose sistemose. Paskutinė el. balsavimo fazė, kuri svarbi vartotojui kaip sistemos patikimo veikimo garantas yra auditas. Abi sistemos naudoja log failuose išsaugotą informaciją, auditui atlikti. Be to, Šveicarijos el. balsavimo sistema naudoja išorinį auditą, kai įtraukiami politinių partijų kontrolieriai, kurie testuoja sistemą. Apžvelgus šiame skyriuje gautus rezultatus bus sprendžiami tolimesni darbo uždaviniai. Bus siekiama pasiūlyti specializuotą pasitikėjimą elektroninėmis balsavimo sistemomis kuriantį modelį.

2. SIŪLOMO SPRENDIMO METODIKA

Šiame skyriuje remiantis atlikta analize siekiama spręsti darbo uždavinį - pasiūlyti specializuotą pasitikėjimą elektroninėmis balsavimo sistemomis kuriantį modelį. Visų pirma atliekama papildoma pasitikėjimą lemiančių veiksnių analizės sistemose apžvalga. Aprašomi pasitikėjimą lemiantys veiksniai bei pačio modelio aprašymas.

2.1 Rinkėjų pasitikėjimą lemiančių veiksnių analizė sistemose

Išnagrinėjus Lietuvos, Estijos bei Šveicarijos el. balsavimo sistemas bei teorinius pasitikėjimą kuriančius modelius buvo nustatyti rinkėjų pasitikėjimą lemiantys veiksniai. Siūloma sistema turi atsakyti ir į rinkėjų pasitikėjimą lemiančius veiksnius.

8 lentelė

Pasitikėjimą lemiančių veiksnių el. balsavimo sistemose palyginimas

Rinkėjų pasitikėjimą lemiantys veiksniai	Lietuvos el. balsavimo sistemos teorinis modelis	Estijos el. balsavimo sistema	Šveicarijos el. balsavimo sistema
<p>Sistemos tikslumas: rinkėjas, dalyvaujantis rinkimuose identifikuoja mas kaip asmuo, kuris jis skelbiasi esąs.</p>	<p>*Skaitmeninio parašo naudojimas (ateityje);</p> <p>*Banko kodų generatorių ar slaptažodžių kortelės panaudojimas prisijungimui prie VRK serverio;</p> <p>*Užšifruota banko pasirašyta informacija apie klientą perduodama į VRK serverį;</p> <p>* VRK serveris, patikrina, ar toks rinkėjas yra rinkimų sąrašuose. Po patikrinimo, VRK sistema rinkėjo „paklausia“, ar tai tikrai tas rinkėjas, kuris prisistato.</p>	<p>*Rinkėjas identifikuoja save su ID kortele;</p> <p>*BPS suformuoja užklausą naudodamas rinkėjo asmeninį identifikacijos kodą iš rinkėjų duomenų bazės, patikrina jo legalumą balsuoti ir nustato jo rinkimų apygardą.</p> <p>*VS užšifruoja pasirinkimą su BSA VR.</p> <p>*Rinkėjas pasirašo kriptogramą SP;</p>	<p>*Skaitmeninio parašo panaudojimas (ateityje);</p> <p>*16 skaitmenų balsavimo kortelės numeris, kuris keičiamas kiekvienų rinkimų metu ir parenkamas kiekvienam rinkėjui atsitiktinai;</p> <p>*Rinkėjai identifikuojami pagal gimimo datą ir vietą;</p> <p>*Sistema blokuoja kortelę po 5 nesėkmingų prisijungimo bandymų;</p>

8 lentelės tęsinys

Rinkėjų pasitikėjimą lemiantys veiksniai	Lietuvos elektroninio balsavimo sistemos teorinis modelis	Estijos elektroninio balsavimo sistema	Šveicarijos elektroninio balsavimo sistema
<p>Sistemos skaidrumas: rinkėjai privalo žinoti, jog jų balsai bus įskaičiuoti į galutinį rezultatą.</p>	<p>*Konceptijoje numatytas saugus ryšio kanalas; *VRK serveris patikrina, ar prisijungęs rinkėjas yra rinkimų sąrašuose; *Rinkėjas priskiriamas atitinkamai rinkimų apygardai.</p>	<p>*Saugus ryšio kanalas; *Žinutė informuoja rinkėją.</p>	<p>*SSL gali būti patikrintas rinkėjo naudojant jo piršto antspaudą. *Realizuotas puslapis, kuriame rinkėjas gali pasitikrinti ar sistema priėmė jo balsą.</p>
<p>Pakartotinis balsavimas: rinkėjo balsas gali būti įskaičiuotas į galutinį balsų skaičiavimą tik vieną kartą.</p>	<p>*Rinkėjo balsas VRK serveryje nedelsiant užkoduojamas ir patenka į el. balsadėžę; *Rinkėjų sąraše pažymima, kad rinkėjas balsavo, o užkoduotas balsas su rinkėjo identifikacijos duomenimis patenka į el. balsadėžę, kur yra saugomas iki tradicinio balsavimo pabaigos.</p>	<p>*Dvigubi balsai atšaukiami; *Balsų skaičiavimas vyksta BSS, atskirtame nuo išorės; *Sistemos privatus raktas yra aktyvuojamas rakto vadybininkų; *Balsavimo skaičiavimo įeinantys duomenys yra balsai paimti iš BSS išorinėje laikmenoje ir surūšiuotoje pagal balsavimo apygardas.</p>	<p>*Įgaliojimų nutraukimas, priėjimui prie balso, kai tik jis registruojamas el. balsavimo dėžėje; *Aiškūs ženklai ant balsavimo voko (nenulaužiamas antspaudas per slaptą priėjimo kodą), parodantis, kad rinkėjas jau balsavo elektroniniu būdu.</p>
<p>Rinkėjų konfidencialumas: rinkėjo pasirinkimas turi išlikti slaptas.</p>	<p>*Pasibaigus rinkimų dienai, el. balsadėžėje esantys balsai atskiriami nuo rinkėjo tapatybės duomenų, išrūšiuojami pagal apygardas ir iššifruojami; *El. balsadėžės balsai iššifruojami naudojant sudėtingą fragmentuotą šifrą, kurio skirtingus fragmentus turi skirtingi Vyriausiosios rinkimų komisijos nariai.</p>	<p>*Po dvigubų balsų atšaukimo elektroniniu būdu balsavusių rinkėjų sąrašai yra sukompiliuojami ir siunčiami į balsavimo stotis tuo pačiu metu kaip ir išankstinių rinkimų vokai; *Balsų skaičiavimas vyksta BSS, atskirtame nuo išorės. *BSS saugomi užšifruoti kandidatų numeriai, nuo kurių nuimti skaitmeniniai parašai ir sąrašai rinkėjų, kurie balsavo el. balsavimo metu.</p>	<p>*Atskirai saugoma asmeninė informacija ir rinkėjo specialios detalės. *Nuolatinis maišymas el. balsavimo sistemos siekiant atsitiktinio generatoriaus; *Kiekvienas balsas užšifruotas dviem šifravimo raktais, tiekiamais šalių kontrolierių. Be raktų balsų skaičiavimas negalimas. *Kiekvienas biuletenio balsas yra konvertuojamas į paveiksluką. Taip sukuriamas dviguba šifravimo procedūra.</p>

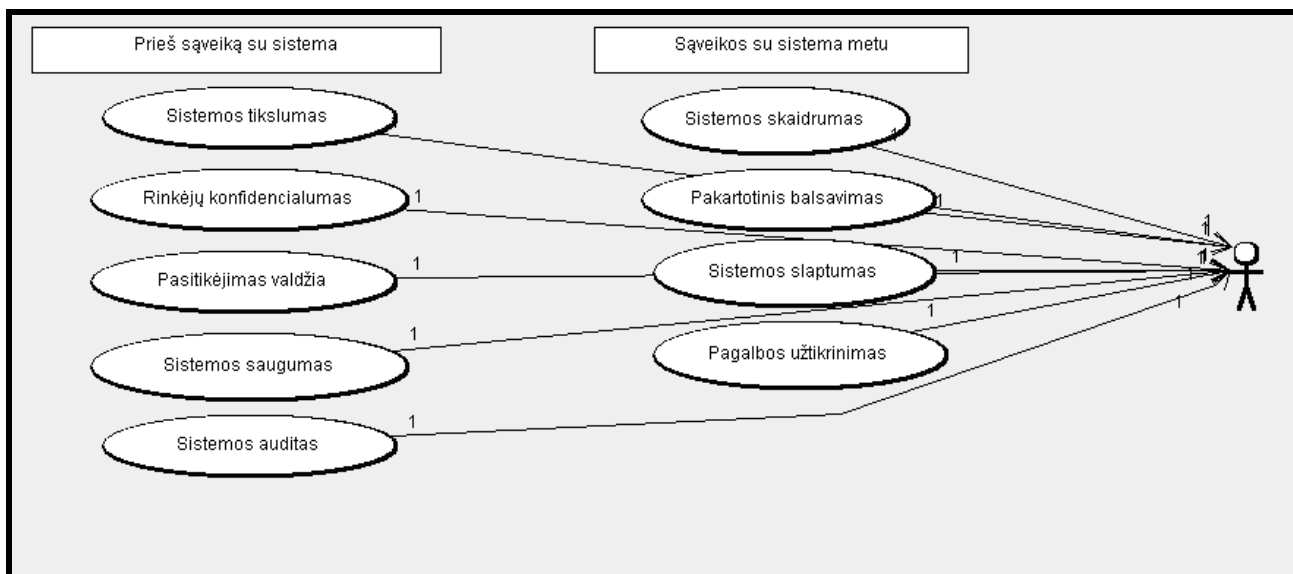
8 lentelės tęsinys

Rinkėjų pasitikėjimą lemiantys veiksniai	Lietuvos el. balsavimo sistemos teorinis modelis	Estijos el. balsavimo sistema	Šveicarijos el. balsavimo sistema
<p>Sistemos slaptumas: Balso perdavimas nuo vartotojo sąsajos iki BPS: perdavimo kanalas tarp rinkėjo ir serverio turi būti saugus, rinkėjai turi būti tikri, kad jų balsai nusiųsti į oficialų serverį ir, kad balsai apsaugoti nuo trečiosios šalies priėjimo</p>	<p>*Konceptijoje numatytas saugus ryšio kanalas; *Viešojo rakto kriptografinis metodas; *El. balsadėžės balsai iššifruojami naudojant sudėtingą fragmentuotą šifrą, kurio skirtingus fragmentus turi skirtingi Vyriausiosios rinkimų komisijos nariai.</p>	<p>*Dvigubas šifravimas (viešuoju raktu pažymėti balsai) pasirašomi skaitmeniniu parašu; * Raktų pora yra generuojama Techninės įrangos saugumo modulyje, privatus raktas, niekada neišimamas iš šio modulio.</p>	<p>*Balso detalės perduodamos grafiškai; *Visi gaunami paketai testuojami dėl jų integralumo, naudojant horizontalias kontrolines sumas. * SSL protokolas komunikacijai; * Balsai yra apsaugomi užšifruojant viešuoju raktu; *Privatų raktą turi tik kontrolieriai ir jie gali dešifruoti balsus jų skaičiavimo metu, po rinkimų uždarymo.</p>
<p>Sistemos saugumas: Apsauga nuo išorinių atakų: galutinio vartotojo įrenginiai (personaliniai kompiuteriai, mobilūs telefonai) galimas balsų perėmimas ir pakeitimas.</p>	<p>*Konceptijoje neatsižvelgta į galutinius vartotojo įrenginius, jų saugumas nenumatytas.</p>	<p>*VA veikia internetiniame puslapyje. Pasirašytas ActiveX apletas yra įkeliamas į vartotojo naršyklę.</p>	<p>*Sudėtinė apsauga ugniasienių pagalba; *Balsavimo kodo metodai (Ciuricho SMS, balso perdavimas ryšio kanalu kaip skaičių seka); *Antivirusinių programų panaudojimas.</p>
<p>Pagalbos užtikrinimas – vartotojui užtikrinamos pagalbos lygis, naudojantis el. balsavimo sistema.</p>	<p>* Konceptijoje neaprašyta</p>	<p>* DUK *Telefono linija * Bandomoji versija</p>	<p>* DUK *Telefono linija</p>
<p>Pasitikėjimas valdžia - rinkėjų nuostatos, pasitikėjimas valdžia.</p>	<p>*Neatsižvelgiama.</p>	<p>* Neatsižvelgiama.</p>	<p>* Neatsižvelgiama, tačiau remiantis jau įvykusiais rinkimais, pakankamai aukštas.</p>
<p>Auditas – procedūra užtikrinanti, kad sistema veikia pagal numatytus reikalavimus ir atlieka savo funkcijas be klaidų.</p>	<p>*Pakartotinis balsų perskaičiavimas.</p>	<p>*Pakartotinis balsų perskaičiavimas. * Log failuose išsaugota informacija</p>	<p>*Pakartotinis balsų perskaičiavimas. * Bandomasis balsavimas</p>

Šaltinis: sudaryta autoriaus

2.2 Rinkėjų pasitikėjimą lemiantys veiksniai

Rinkėjų pasitikėjimą lemiantys veiksniai pavaizduoti 7 pav.:



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 38.

7 pav. Pasitikėjimo el. balsavimo sistema elementai.

1. **Sistemos tikslumas** – išreikštas per patikimą autentifikaciją, kuomet asmuo, dalyvaujantis rinkimuose identifikuojamas kaip asmuo, kuris jis skelbiasi esąs. Tik asmenys, turintys teisę balsuoti gali dalyvauti rinkimuose ir asmenys neturintys teisės balsuoti negali dalyvauti rinkimuose. Nagrinėtose sistemose vykdomas skirtingai, tačiau saugiausias iš jų ID kortelės su skaitmeniniu parašu panaudojimas.
2. **Sistemos skaidrumas** - rinkėjai privalo žinoti, jog jų balsai bus įskaičiuoti į galutinį rezultatą. Sistemoje realizuojamas atsiunčiant patvirtinimą apie balso užregistravimą bei sukuriant patogią informatyvią pakartotinio prisijungimo posistemę.
3. **Pakartotinis balsavimas** – realizuotas pakartotinis balsavimas rinkėjui pakeitus pasirinkimą, tačiau užtikrinamas prieš tai buvusio balso išėmimas iš sistemos ir rinkėjo balsas gali būti įskaičiuotas į galutinį balsų skaičiavimą tik vieną kartą. Prieš balsuojant rinkėjas balsavimo puslapyje aiškiai informuojamas, kad balsuoti galima daugiau nei vieną kartą, pakeitus apsisprendimą.
4. **Rinkėjų konfidencialumas** - rinkėjo asmenybė bei pasirinkimas turi išlikti slaptas. Realizuota atskirai saugant rinkėjo asmeninę informaciją ir balsą. Be to atskirtų balsų bei rinkėjų ID sąrašai Balsus saugančiame serveryje sumaišomi siekiant atsitiktinio generavimo bei siekiant nutraukti bet kokius mėginimus susieti šiuos du sąrašus.

5. **Sistemos saugumas** - apsauga nuo išorinių atakų bei galimas balsų perėmimas ir pakeitimas. Perdavimo kanalas tarp rinkėjo ir serverio turi būti saugus, rinkėjai turi būti tikri, kad jų balsai nusiųsti į oficialų serverį ir, kad balsai apsaugoti nuo trečiosios šalies priėmimo. Šifravimui naudojami kriptografiniai metodai bei saugus ryšio kanalo panaudojimas balso perdavimui.
6. **Sistemos slaptumas** - rinkėjų pasirinkimas nebus atskleistas jokiais aplinkybėmis. Realizuotas panaudojant jau minėtas saugumo priemones bei dešifravimui reikalingą privatų raktą padalinus tarp įgaliotų rinkimų komisijos atstovų.
7. **Pagalbos užtikrinimas** – vartotojui užtikrinamos pagalbos lygis, naudojantis el. balsavimo sistema.
8. **Pasitikėjimas valdžia** – rinkėjų nuostatos, pasitikėjimas valdžia. Suprantamas, kaip sistemos kūrėjo įvaizdžio problemos dalis. Gali būti realizuota suteikiant išsamią informaciją apie sistemos kūrėją – valdžios instituciją.
9. **Auditas** – procedūra užtikrinanti, kad sistema veikia pagal numatytus reikalavimus ir atlieka savo funkcijas be klaidų. Kraštutinis audito pavyzdys gali būti pakartotinis balsų perskaičiavimas.

2.3 Pasitikėjimą didinantis el. balsavimo sistemos modelis

Šiame skyrelyje apžvelgiamas pasiūlytas modelis, kurio esminis skirtumas nuo esamų modelių yra pasitikėjimo elementų identifikavimas ir įjungimas į el. balsavimo scenarijaus etapus. Modelis sukurtas remiantis nagrinėtomis Estijos bei Šveicarijos el. balsavimo sistemomis bei pritaikant nagrinėtoje literatūroje apibendrintą el. balsavimo sistemos pasitikėjimo modelį. Ši sistema susideda iš vartotojo sąsajos, tinklo serverio bei serverių, kurie saugo, apdoroja bei skaičiuoja balsus. El. balsavimo sistemoje vykstančius procesus galima suskirstyti į šešis pagrindinius etapus: registraciją, autentifikaciją, balsavimą ir balsų saugojimą, balsų tvarkymą, balsų skaičiavimą bei auditą (Naveed, Z. Ch.; Pilkjaer, A. (2007)). Balsuojančio asmens registracija yra fazė apibrėžianti balsuojančius asmenis elektroninio balsavimo sistemai ir duodanti jiems autentifikavimo duomenis prisijungimui prie elektroninio balsavimo sistemos. Autentifikacija yra fazė patikrinanti ar balsuojantys asmenys turi priėjimo teises ir balsavimo teisę. Balsavimas ir balsų saugojimas yra fazė, kur balsavimo teisę turintys asmenys balsuoja ir elektroninio balsavimo sistema saugoja priimtus iš rinkėjų balsus. Balsų valdymas yra fazė, kurioje balsai yra valdomi, rūšiuojami ir paruošiami skaičiavimui. Balsų skaičiavimas yra fazė, kur balsai yra dešifruojami ir skaičiuojami tam, kad išduoti galutinį rezultatą. Auditas yra fazė tikrinanti ar galintys balsuoti asmenys galėjo balsuoti ir ar jų balsai dalyvavo galutiniame skaičiavime (Ramonaitė, A. (2008)). Pasiūlyto modelio struktūra pateikta 8 pav.

Pasitikėjimą kuriantys elementai: (1) **Sistemos tikslumas** – išreikštas per patikimą **autentifikaciją**, kuomet asmuo, dalyvaujantis rinkimuose identifikuojamas kaip asmuo, kuris jis skelbiasi esąs. Tik asmenys, turintys teisę balsuoti gali dalyvauti rinkimuose ir asmenys neturintys teisės balsuoti negali dalyvauti rinkimuose. Nagrinėtose sistemose vykdomas skirtingai, tačiau saugiausias iš jų ID kortelės su skaitmeniniu parašu panaudojimas. (2) **Sistemos skaidrumas** - rinkėjai privalo žinoti, jog jų balsai bus įskaičiuoti į galutinį rezultatą. Sistemoje realizuojamas atsiunčiant bei sukuriant informatyvią pakartotinio prisijungimo posistemę. (3) **Pakartotinis balsavimas** – realizuotas pakartotinis balsavimas rinkėjui pakeitus pasirinkimą, tačiau užtikrinamas prieš tai buvusio balso išėmimas iš sistemos ir rinkėjo balsas gali būti įskaičiuotas į galutinį balsų skaičiavimą tik vieną kartą. Prieš balsuojant rinkėjas balsavimo puslapyje aiškiai informuojamas, kad balsuoti galima daugiau nei vieną kartą, pakeitus apsisprendimą. (4) **Rinkėjų konfidencialumas** – balsus skaičiuojančiame serveryje atskirai saugoma rinkėjo asmeninė informacija bei jo balsas. Be to atskirtų balsų bei rinkėjų ID sąrašai nuolatos maišomi siekiant atsitiktinio generavimo bei siekiant nutraukti bet kokius mėginimus susieti šiuos du sąrašus. 5)

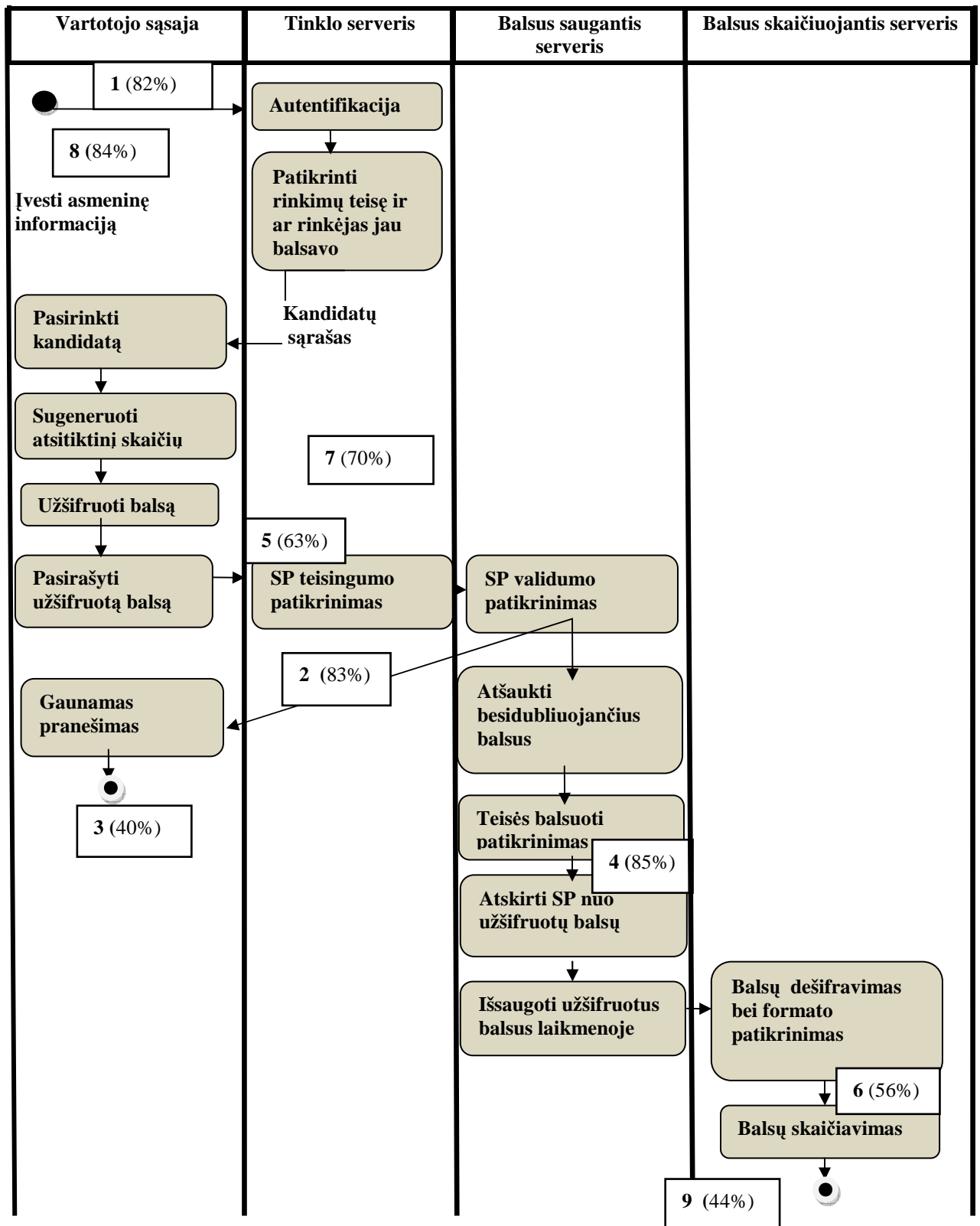
Sistemos saugumas - perdavimo kanalas tarp rinkėjo ir serverio turi būti saugus, rinkėjai turi būti tikri, kad jų balsai nusiųsti į oficialų serverį ir, kad balsai apsaugoti nuo trečiosios šalies priėjimo. Šifravimui naudojami kriptografiniai metodai bei saugaus ryšio kanalo panaudojimas balso perdavimui. Reikalingi dėl to, kad rinkėjai jaustųsi saugūs pateikdami savo pasirinkimą. (6)

Sistemos slaptumas - rinkėjų pasirinkimas nebus atskleistas jokiais aplinkybėmis. Realizuotas panaudojant jau minėtas saugumo priemones bei dešifravimui reikalingą privatų raktą padalinus tarp įgaliotų rinkimų komisijos atstovų. Apie šią el. balsavimo sistemos veikimo dalį, rinkėjai turi būti informuojami prieš balsavimo procesą. (7)

Pakankamos pagalbos rinkėjams užtikrinimas: pagalba išdėstyta patogiai lange, į ją kreipiamasi bet kuriuo metu, be to, rinkėjas gali grįžti atgal visame balsavimo procese. Reikalinga dėl sistemos suprantamumo ir adaptavimo rinkėjui. (8)

Pasitikėjimas valdžia - išsami informacija apie sistemos kūrėją, atvaizduojama vartotojo sąsajoje prieš autentifikaciją. Jis yra svarbus kaip institucinis požymis, veikiantis piliečio elgesį bei apsiprendimą. (9)

Auditas - informacija, kad sistema audituojama viso proceso metu. Reikalinga dėl sistemos patikimumo. Informavimas apie balsų perskaičiavimo galimybę. Balsai saugomi ir prireikus perskaičiuojami, užtikrinamas papildomas sistemos auditas.



Šaltinis: sukurta autoriaus pagal MAGI, T. (2007) Practical Security Analysis of E-voting Systems; KRIMMER, R. (2004) How Security problems Can Compromise Remote Internet Voting Systems.

8 pav. Pasitikėjimą didinantis el. balsavimo sistemos modelis.

2.4 Siūlomo sprendimo metodikos skyriaus išvados

Apibendrinus Šveicarijos bei Estijos el. balsavimo sistemas bei atlikus teorinių modelių analizę buvo pasiūlytas pasitikėjimą el. balsavimo sistemomis kuriantis modelis. Jis apima devynis pagrindinius elementus, kurie remiantis atlikta analize turi įtakos rinkėjo pasitikėjimui. Pasitikėjimą kuriantys elementai: 1) **Sistemos tikslumas** yra išreikštas per patikimą autentifikaciją, rinkėjas identifikuojamas kaip asmuo, kuris jis skelbiasi esąs. 2) **Sistemos skaidrumas** – rinkėjo informavimas apie jo balso įskaičiavimą į galutinį rezultatą. Sistemoje realizuojamas atsiunčiant pranešimą bei sukuriant informatyvią pakartotinio prisijungimo posistemę. 3) **Pakartotinis balsavimas** – realizuotas pakartotinis balsavimas rinkėjui pakeitus pasirinkimą, tačiau užtikrinama, kad rinkėjo balsas gali būti įskaičiuotas į galutinį balsų skaičiavimą tik vieną kartą. 4) **Rinkėjų konfidencialumas** – balsus skaičiuojančiame serveryje atskirai saugoma rinkėjo asmeninė informacija bei jo balsas. Be to atskirtų balsų bei rinkėjų ID sąrašai nuolatos maišomi siekiant atsitiktinio generavimo bei siekiant nutraukti bet kokius mėginimus susieti šiuos du sąrašus. 5) **Sistemos saugumas** - perdavimo kanalas tarp rinkėjo ir serverio turi būti saugus, rinkėjai turi būti tikri, kad jų balsai nusiųsti į oficialų serverį ir, kad balsai apsaugoti nuo trečiosios šalies priėjimo. Šifravimui naudojami kriptografiniai metodai bei saugaus ryšio kanalo panaudojimas balso perdavimui. 6) **Sistemos slaptumas** - rinkėjų pasirinkimas nebus atskleistas jokiais aplinkybėmis. Realizuotas panaudojant jau minėtas saugumo priemones bei dešifravimui reikalingą privatų raktą padalinus tarp įgaliotų rinkimų komisijos atstovų. 7) **Pakankamos pagalbos** rinkėjams užtikrinimas: pagalba išdėstyta patogiai lange, į ją kreipiamasi bet kuriuo metu, be to, rinkėjas gali grįžti atgal visame balsavimo procese. 8) **Pasitikėjimas valdžia** - išsami informacija apie sistemos kūrėją, atvaizduojama vartotojo sąsajoje prieš autentifikaciją. Jis yra svarbus kaip institucinis požymis, veikiantis piliečio elgesį bei apsiprendimą. 9) **Auditas** yra reikalingas dėl sistemos patikimumo. Informavimas apie balsų perskaičiavimo galimybę.

3. EKSPERIMENTINIS SKYRIUS

Ekspérimentiniame skyriuje siekiama pasirinkti tinkamas priemones pateikto koncepcinio modelio tinkamumui patikrinti (Šarkiūnaitė, D.; Krikščiūnienė, D.; Simutis, R. (2007)). Atsižvelgiant jame aprašomas duomenų rinkimas, duomenų apdorojimas ir analizė, rezultatų analizė, interpretavimas ir apibendrinimas bei išvados.

3.1 Duomenų rinkimas

Duomenų rinkimui buvo sudaryta anketa iširti respondentų požiūrį į el. balsavimo sistemas (Priedas 2, Priedas 1). Atliekant tyrimą dalyvavimo statusas turi būti apibrėžtas labai tiksliai, nes jis įtakoja tyrėjo išvadų patikimumą. Atsižvelgiant į tyrimo sritį — elektroninę vyriausybę ir tiksliau el. balsavimą, galima teigti, jog tyrėjas yra dalinai dalyvaujantis stebėtojas, kadangi jis yra subjektyvus (turi savo asmeninę nuomonę) bei objektyvus (remiasi moksliniais šaltiniais). Tiriamieji buvo visi Aalborg universiteto studentai, įvairių tautybių, amžiaus, lyties bei skirtingo naudojimosi kompiuteriu lygio.

- Patikimumas – siekia atsakyti į klausimą ar tyrimo rezultatai gali būti pakartoti. Siekiant patvirtinti tyrimo patikimumą reikalinga atsakyti į klausimą ar tyrimo metu atliktas matavimas yra stabilus ar ne. Ar rezultatai nuoseklūs? (Bryman, A.; Bell, E. (2007)). Patikimumas gali būti nustatytas tik pakartotinio tyrimo metu, imant tą pačią tiriamąją imtį. Tačiau dėl resursų stokos pakartotinis matavimas nebuvo atliktas.
- Pakartojamumas priežastys gali būti įvairios, pvz. originalūs tyrimo rezultatai nesutampa su kitu įrodymu, kuris atitinka klausimo sritį. Tyrimas turi būti aprašytas detalčiai, kitu atveju tyrimo pakartojamumas nebus įmanomas. Tuo pačiu, siekiant įvertinti tyrimo pakartojamumą, procedūros, kurios matuoja pakartojamumą turi būti apibrėžtos kito tyrėjo (Bryman, A.; Bell, E. (2007)). Šio tyrimo atveju, pakartojamumas yra įmanomas, nes tyrimas aprašytas pakankamai išsamiai ir aiškiai.
- Validumas yra svarbiausias tyrimo kriterijus.
 - a) Matavimo validumas siekia atsakyti į klausimą: ar priemonė, kuri yra sukurta sąvokos pagalba tikrai atspindi sąvoką, kurią ji turi pažymėti. Jei tyrimo matavimas nevalidus, tyrimo rezultatai bus abejotini. Matavimo validumo įvertinimas lemia ar priemonė yra patikima (Bryman, A.; Bell, E. (2007)). Ar tikrai atliekamas tyrimas matuoja pasitikėjimą el. balsavimo sistemomis? Galima teigti, kad taip, nes prieš tyrimą buvo atlikta išsami mokslinių šaltinių analizė ir anketa sudaryta remiantis šioje analizėje gautais rezultatais.

b) Išorinis validumas apibrėžia ar tyrimo rezultatai gali būti apibendrinti už specifinio tyrimo konteksto ribų. Tampa svarbu kaip buvo parinkti tyrimo objektai ir aplinka (Bryman, A.; Bell, E. (2007)). Galima teigti, kad tyrimo rezultatai gali būti apibendrinti ir už tyrimo konteksto ribų, nes tyriamoji imtis yra pakankamai plati bei įvairi.

c) Ekologinis validumas siekia atsakyti ar socialiniai moksliniai atradimai yra taikytini kasdieniniame gyvenime, natūraliuose socialiniuose nustatymuose. Atliktas tyrimas gali būti validus techniškai, tačiau neturi nieko bendro su kasdieniniu gyvenimu. Tyrimo aplinka turi būti natūrali, įprasta respondentui (Bryman, A.; Bell, E. (2007)). Šio tyrimo atveju, respondentai buvo apklausiami jiems natūraliose sąlygose, todėl išoriniai trikdžiai nepadarė neigiamos įtakos.

3.2 Tyrimo vieta, laikas, pradžios ir pabaigos datos

Tyrimo vieta: Aalborg miestas, Danija

Tyrimo laikas: 2 mėn.

Tyrimo pradžia: 2008-12-01

Tyrimo pabaiga: 2009-01-31

3.3 Tyrimo apribojimai

Tyrimui trukdė nepakankamas žinių bei tyrimų atlikimo įgūdžių lygis. Sudarytos anketos klausimai galėjo būti interpretuoti skirtingai, nes respondentai atsakinėjo subjektyviai. Kiekvienas asmuo turi savo pradines nuostatas, išsilavinimą bei žinių lygį.

3.4 Duomenų apdorojimas ir analizė

Šioje dalyje sukurti metodai, algoritmai, procedūros ar specifinė veiksmų seka, skirta duomenims apdoroti ir tirti yra aptariama. Tyrimas remiasi atvejų analize – egzistuojančių el. balsavimo sistemų analize. Pagal ištirtas sistemas buvo sudarytas preliminarus pasitikėjimą lemiančių veiksnių sąrašas.

1. Sudaryta anketa ir ištirti Aalborg universiteto studentai.

Klausimai nuo 1-5 klausimyne sudaryti siekiant nustatyti socialinį respondento profilį: lytis, amžius, gyvenamoji vieta, išsilavinimas, naudojimosi kompiuteriu lygis. Klausimai 6-7 siekia nustatyti kokias el. valdžios paslaugas respondentas naudoja. Klausimai 8 bei 9 siekia

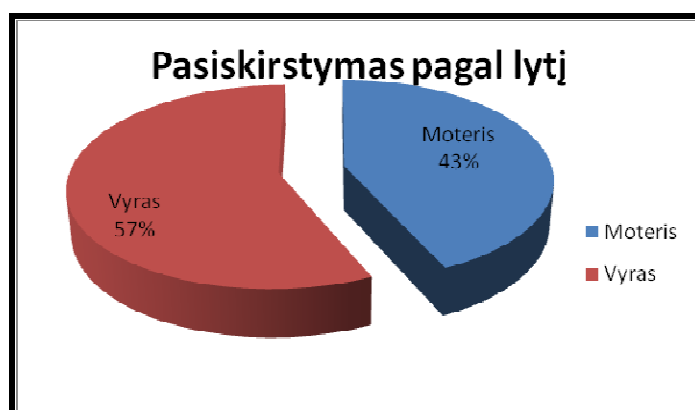
išsiaiškinti respondento pasitenkinimą dabartine balsavimo sistema ir jo argumentus dėl el. balsavimo sistemos. Tolimesni klausimai siekia išsiaiškinti, kurie faktoriai el. balsavimo sistemoje svarbūs rinkėjui ir kurie nedaro jokios įtakos. Tyrimas atliktas, panaudojant 25 klausimus struktūrizuotu klausimynu (Priedas Nr. 1, 2). Klausimynas sudarytas laikantis klausimyno sudarymo principų. Anketos pradžioje nurodytas tyrimo tikslas, respondentas supažindintas su keliamos problemos aktualumu, nurodyta, jog anketa yra anoniminė, o duomenys bus naudojami apibendrintai. Anketoje nurodyta instrukcija, kaip reikia ją pildyti. Taip pat reikia pažymėti, kad respondentas atsako į klausimus kaip rinkėjas. Respondentai atrinkti pasinaudojant netikimybinės atrankos, parankiosios atrankos principu (imtis gaunama tada, kai apklausiami arčiausiai esantys ir lengviausiai prieinami populiacijos elementai).

2. Remiantis gautais rezultatais buvo sureitinguoti pasitikėjimo el. balsavimo sistema veiksniai.

Naudojamos kompiuterizuotos analizės priemonės – Microsoft Office Excel apdoroti anketos rezultatus. El. balsavimo sistemos veikimo diagramos braižomos UML programinių įrankių pagalba. Buvo naudojama ArgoUML 0.28 programinė įranga skirta UML diagramų kūrimui.

3.5 Rezultatų analizė

Šiame poskyryje vykdoma surinktų duomenų esminių temų ar požymių identifikavimas tolimesniam detalesniam ištyrimui. Pagal gautus rezultatus respondentai pagal lytį pasiskirstė apylygiai 57% vyrų ir 43% moterų.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemoje tyrimas, p. 46.

9 pav. Respondentų pasiskirstymas pagal lytį.

Apklausiamieji buvo Aalborg universiteto studentai, todėl pagal amžių didžiausias procentas respondentų buvo 21-25 m., antroje vietoje buvo 26-35 metų žmonės.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektronibalsavimo sistemose tyrimas, p. 47.

10 pav. Respondentų pasiskirstymas pagal amžių.

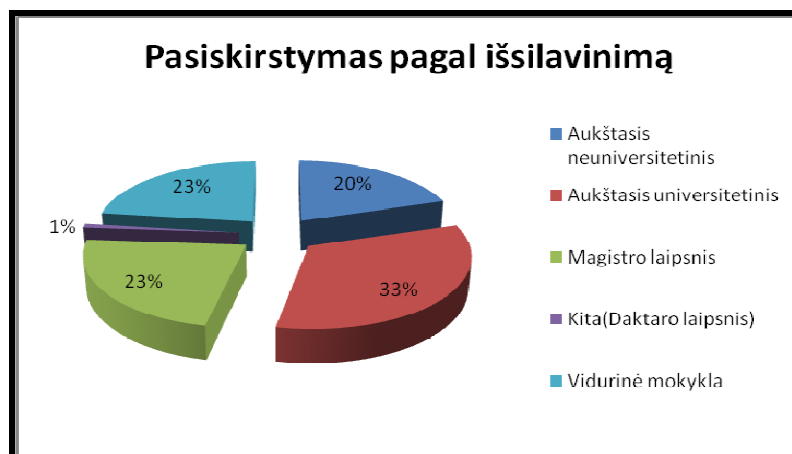
Apklausiamieji buvo skirtingų tautybių bei pastovios gyvenamosios vietos atstovai. Šis klausimas buvo įtrauktas siekiant parodyti, skirtingų šalių požiūrį į el. balsavimą. Kadangi tyrimas buvo atliktas Danijoje, daugiausiai apklaustųjų buvo danai, antroje vietoje lenkai bei lietuviai.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektronibalsavimo sistemose tyrimas, p. 47.

11 pav. Respondentų pasiskirstymas pagal pastovią gyvenamąją vietą.

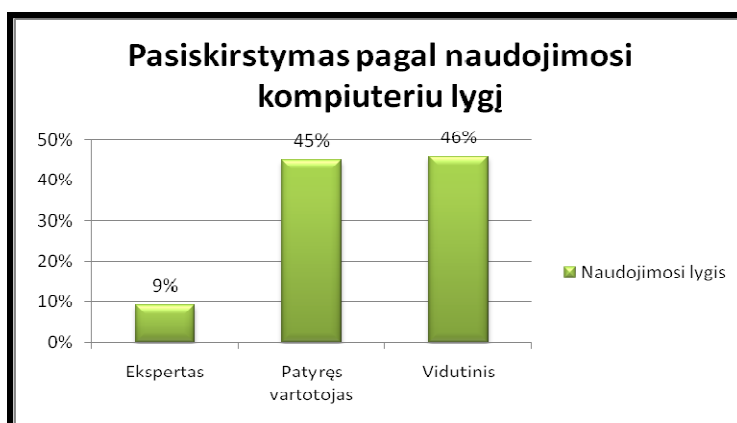
Didžiausia dalis apklaustųjų yra įgiję aukštąjį universitetinį (33%), magistro laipsnį (23%) bei vidurinį išsilavinimą (23%).



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 48.

12 pav. Respondentų pasiskirstymas pagal išsilavinimą

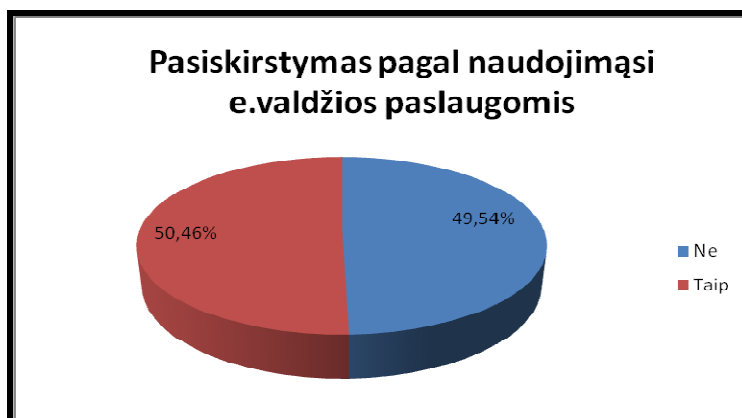
Kaip ir buvo galima tikėtis, respondentai parodė gana aukštą naudojimosi kompiuteriu lygį. Nebuvo nei vieno, kuris būtų atsakęs, kad nesinaudoja kompiuteriu.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 48.

13 pav. Respondentų pasiskirstymas pagal naudojimosi kompiuteriu lygį

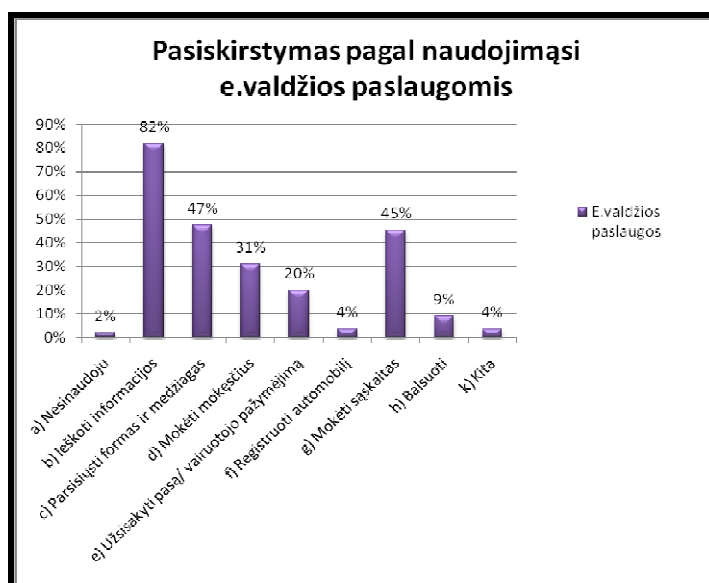
Nors pagal naudojimosi kompiuteriu lygį, respondentai save priskyrė prie vidutinių arba patyrusių vartotojų, tik pusė (50,46%) apklaustųjų naudojami el. valdžios paslaugomis.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 49.

14 pav. Respondentų pasiskirstymas pagal naudojimąsi el. valdžios paslaugomis.

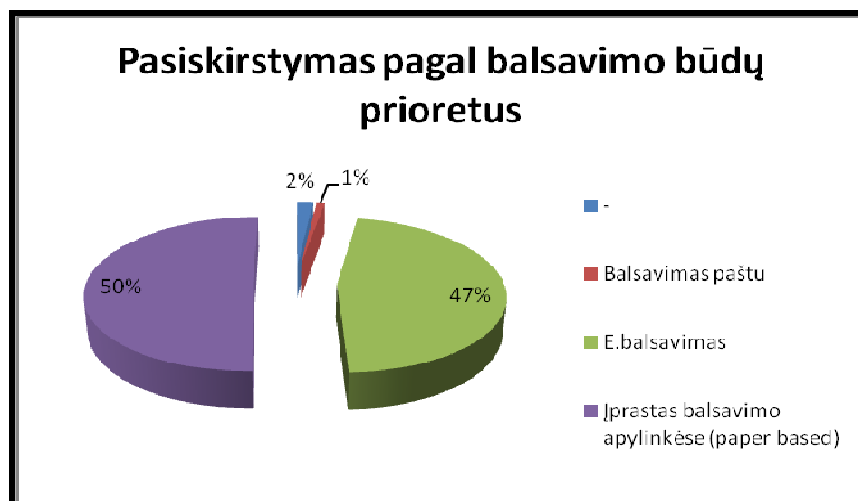
Iš asmenų, kurie atsakė į klausimą apie naudojimąsi el. valdžios paslaugomis teigiamai, populiariausios paslaugos yra: ieškoti informacijos (82%), parsisiųsti formas ir medžiagas (47%) bei mokėti sąskaitas (45%) apklaustųjų.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 49.

15 pav. Pasiskirstymas pagal naudojimąsi skirtingomis el. valdžios paslaugomis.

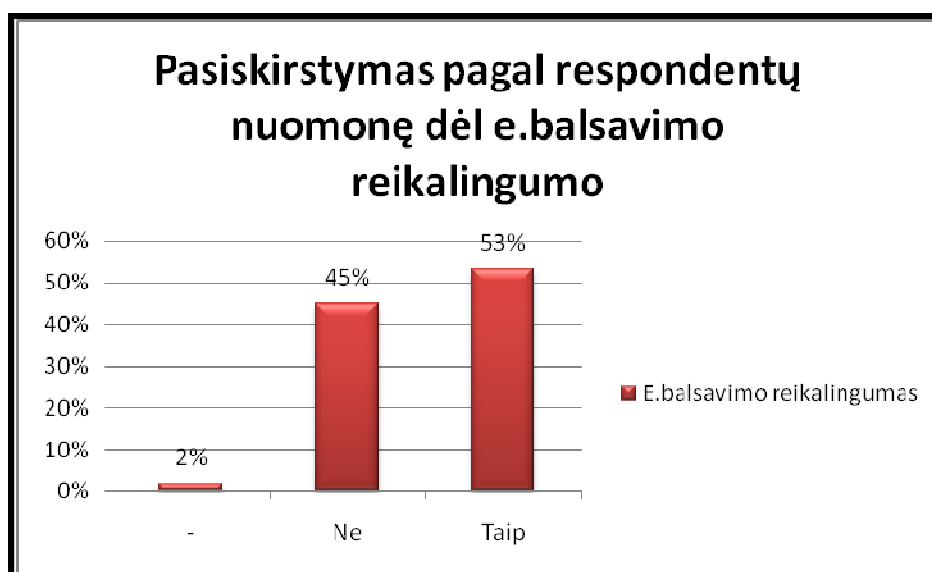
50% apklaustųjų mieliau rinktųsi įprastą balsavimą ir 47% el. balsavimą.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 50.

16 pav. Pasiskirstymas pagal balsavimo būdus

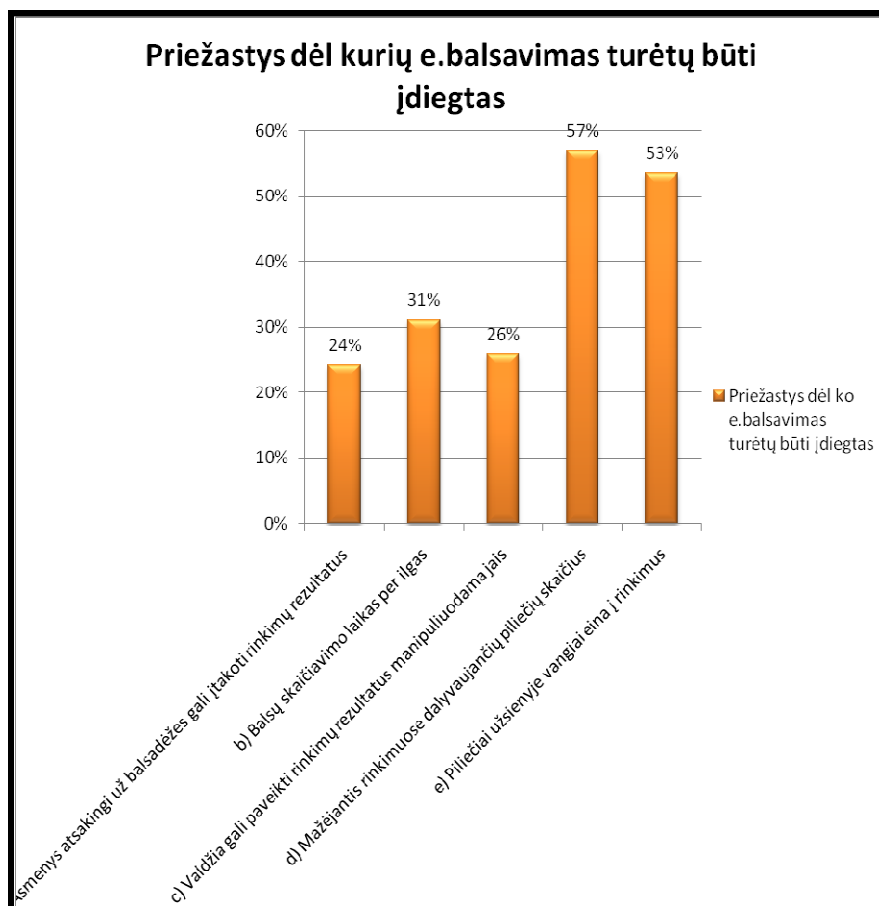
Net (53%) apklaustųjų mano, kad el. balsavimas reikalingas įdiegti jų šalyse.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 50.

17 pav. Pasiskirstymas pagal el. balsavimo reikalingumą respondentų šalyse.

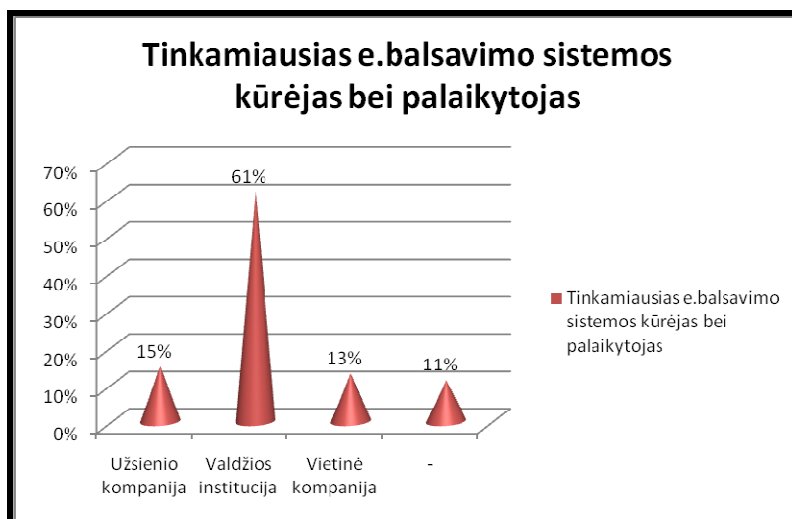
Respondentai daugiausiai mano, kad el. balsavimas turėtų būti įdiegtas dėl mažėjančio rinkimuose dalyvaujančių piliečių skaičiaus (57%) bei piliečių esančių užsienyje vangaus ėjimo į rinkimus (53%).



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 51.

18 pav. Priežastys dėl kurių el. balsavimas turėtų būti įdiegtas.

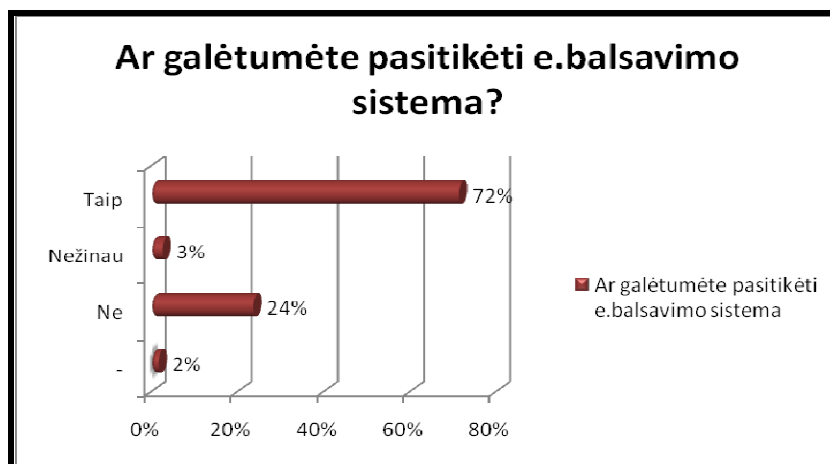
Tinkamiausiu el. balsavimo sistemos kūrėju bei palaikytoju, respondantai laiko valdžios instituciją (61%).



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 52.

19 pav. Tinkamiausias sistemos kūrėjas bei palaikytojas.

Į klausimą „kaip Jūs manote, ar pasitikėtumėte el. balsavimo sistemomis?“ respondentai atsakė labai palankiai el. balsavimo sistemų atžvilgiu, net 72% manė, kad galėtų.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 52.

20 pav. Išankstinis apklaustųjų pasitikėjimas el. balsavimo sistema.

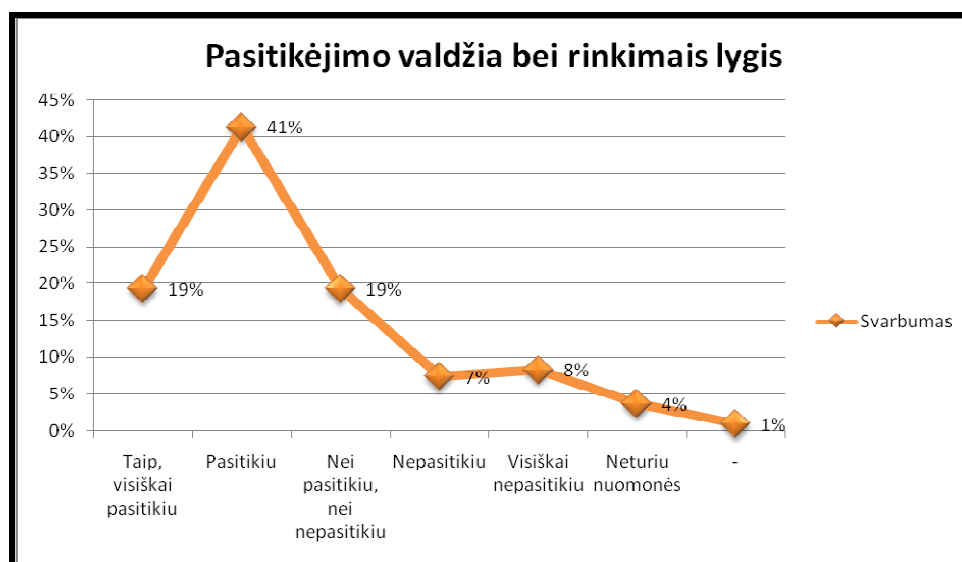
Didžiausią svarbą tarp pasirinktinių rodiklių apklaustieji nurodė rinkėjo konfidencialumą bei autentifikaciją ir pagalbą. Mažiau svarbu buvo pasitikėjimas valdžios insitucijomis bei rinkimais.

Rodiklių, lemiančių pasitikėjimą el. balsavimo sistema pasiskirstymas

	a) Autentifi kacija	b) Sistemos skaidrumas	c) Pakartotin is balsavimas	d) Rinkėjo konfidencial umas	e) Visapusiška pagalba	f) El. bankininkystės panaudojimas el. balsavimo sistemoje	g) Pasitikėjimas valdžios institucijomis ir rinkimais
Taip, labai	57%	31%	12%	68%	60%	13%	50%
Taip	25%	39%	28%	17%	10%	20%	34%
Nei taip, nei ne	6%	15%	22%	6%	12%	32%	9%
Ne	-	2%	16%	4%	13%	10%	1%
Visiškai Ne	-	-	3%	-	-	4%	-
Neturiu nuomonę	7%	8%	15%	3%	2%	17%	2%
-	5%	5%	5%	3%	3%	5%	4%

Šaltinis: sudaryta autoriaus.

Iš 21 pav. matome, kad respondentai linkę pasitikėti valdžia bei rinkimais, aukščiausias procentas respondentų pasitiki valdžia bei rinkimais.

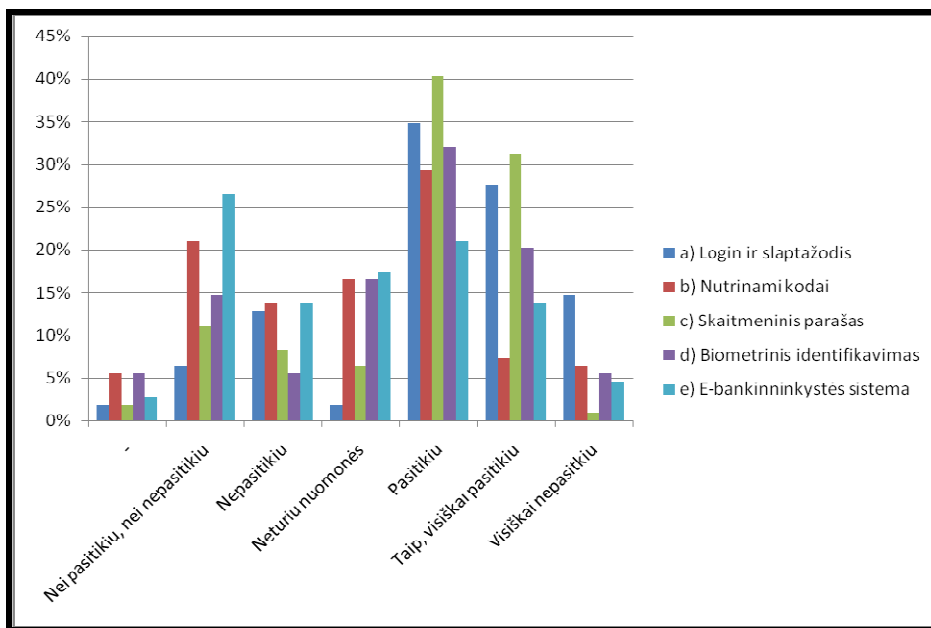


Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 53.

21 pav. Pasitikėjimas valdžia bei rinkimais.

Respondentai labiausiai pasitiki skaitmeniniu parašu (71%), prisijungimo vardu bei slaptažodžiu (63%), biometriniu identifikavimu (52%), nutrinamų kodų kortelė (36%) bei el. bankininkystės sistema (35%). Nors pagal tyrimo rezultatus tinkamiausiai įvertintas skaitmeninis parašas, reikia

įvertinti, kad norint įgyvendinti šį autentifikavimo būdą reikalinga skaitmeninio parašo infrastruktūra.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 54.

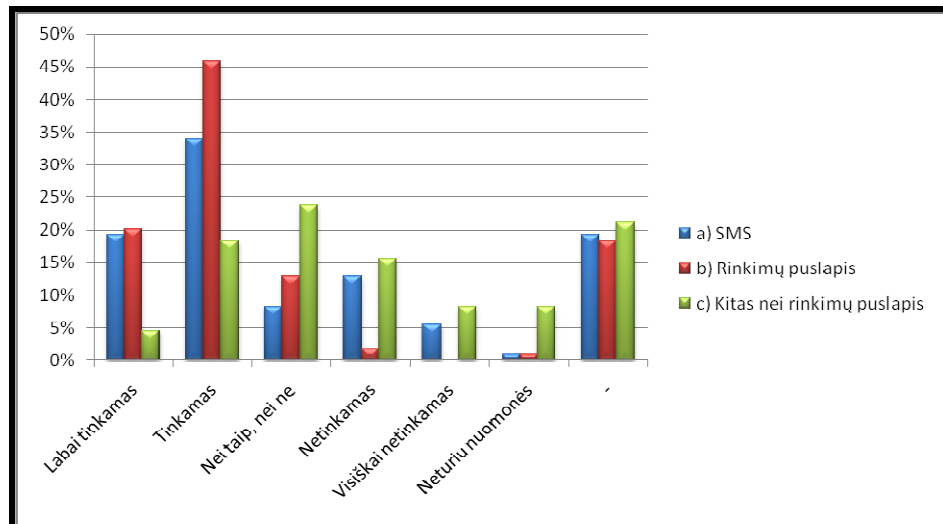
22 pav. Pasitikėjimo elementai autentifikacijos procese.

Kiti respondentų siūlomi būdai buvo: pirštų antspaudai, nuotrauka, vienkartinis slaptažodis bei asmeniniai duomenys reikalingi prisijungimui. Remiantis 23 pav. Rinkėjai labiau pasitikėtų el. balsavimo sistema, jei gautų patvirtinimą apie balso užregistravimą (83%).



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 54.

23 pav. Patvirtinimo apie balso užregistravimą reikalingumas.

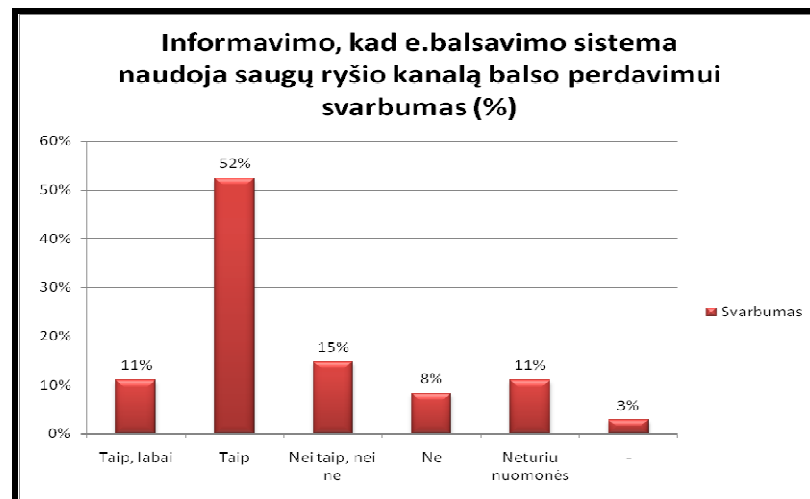


Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 55.

24 pav. Patvirtinimo būdai, kad balsas užregistruotas balsavimo procese.

Priimtinausias būdas patvirtinti, kad balsas buvo užregistruotas yra rinkimų puslapis (66%) apklaustųjų, SMS servisas taip pat priimtinas, bet suteikiantis mažiau pasitikėjimo (53%). Tuo tarpu kitas nei rinkimų puslapis rinkėjams pasitikėjimo nesuteikia, jis įvertintas neigiamai.

Kiti galimi balso užregistravimo pranešimo būdai: „e-mail“, „letter“, „paper“, „printed paper“, „send documents to home adress“ ir „via post“.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 55.

25 pav. Saugaus ryšio kanalo naudojimo balso perdavimui svarbumas.

Remiantis 25 pav. galime daryti išvadas, kad informavimo, kad el. balsavimo sistema naudoja saugų ryšio kanalą balso perdavimui yra labai svarbus pasitikėjimo elementas el. balsavimo sistemoje. Net 63% apklaustųjų mano, kad tai svarbu arba labai svarbu.

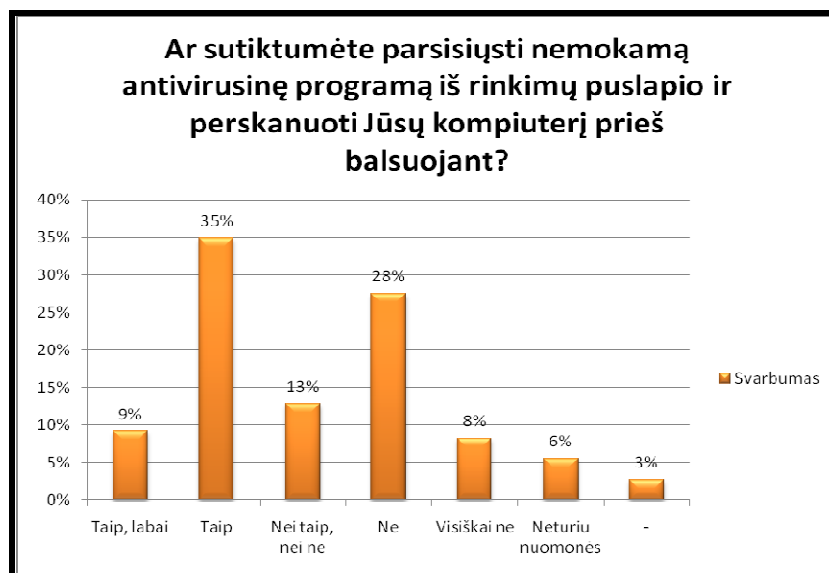


Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 56.

26 pav. Balso užšifravimas perdavimo metu saugiu kriptografiniu metodu

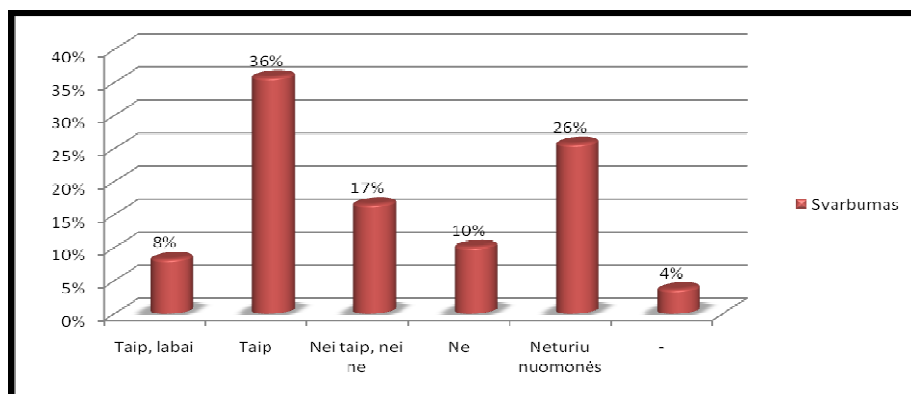
Iš 26 pav. galime daryti išvadas, kad informavimas, jog balsas užšifruotas perdavimo metu saugiu kriptografiniu metodu yra labai svarbus pasitikėjimo elementas el. balsavimo sistemoje. Net 62% apklaustųjų mano, kad tai svarbu arba labai svarbu.

Iš 27 pav. matome, kad respondentai pasiskirstė apylygiai vertindami antivirusinės programos parsisiuntimą iš rinkimų puslapio ir jų kompiuterio perskanavimo galimybę prieš balsuojant.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 56.

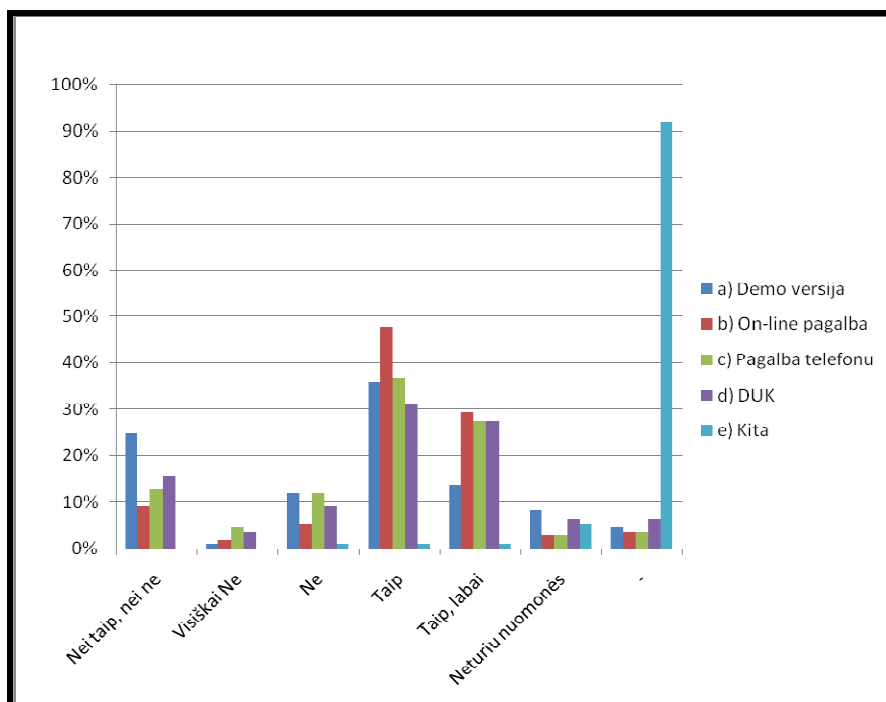
27 pav. Galimybės parsisiųsti nemokamą antivirusinę programą ir perskanuoti kompiuterį pasirinkimas.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 57.

28 pav. Sistemos audito svarbumas.

Iš 28 pav. matome, kad informavimas, jog sistema buvo audituojama veikia rinkėjų pasitikėjimą (44%).



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 57.

29 pav. Pagalbos įrankiai, įtakoiantys rinkėjo pasitikėjimą el. balsavimo sistema.

Tinkamiausia pagalba Online pagalba, pagalba telefonu bei DUK.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 58.

30 pav. Sistemoje realizuoto balsų perskaičiavimo svarbumas

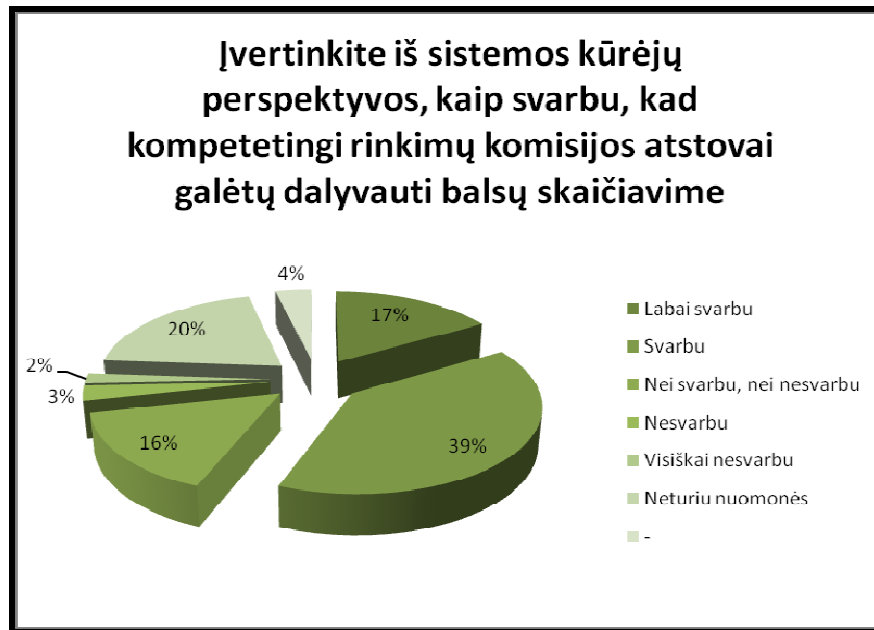
Iš 30 pav. matome, kad balsų perskaičiavimo galimybė rinkėjams yra labai svarbi. Net 66% apklaustųjų mano, kad tai svarbu arba labai svarbu. Rinkėjai turėtų būti informuoti apie balsų perskaičiavimo galimybę prieš balsuojant.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 58.

31 pav. Svarbumas, kad rinkimų balsai nebūtų paviešinti prieš rinkimų pabaigą.

Iš 31 pav. matome, kad faktas, kad balsai negali būti paviešinti prieš rinkimų pabaigą yra labai svarbi. Net 56% apklaustųjų mano, kad tai svarbu arba labai svarbu.



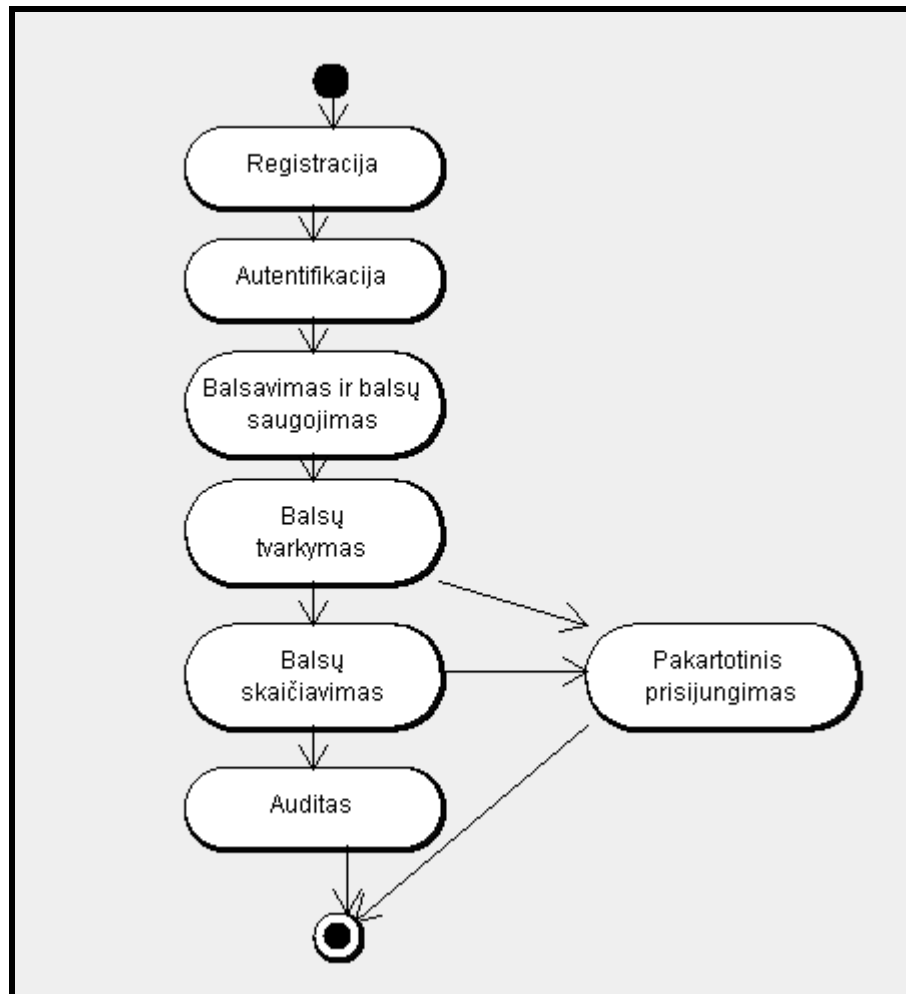
Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 58.

32 pav. Kompetetingų rinkimų komisijos atstovų dalyvavimas balsų skaičiavime

Iš pav. 32 matome, kad faktas, jog kompetetingi rinkimų komisijos atstovai galėtų dalyvauti balsų skaičiavime yra svarbus arba labai svarbus 56% apklaustųjų.

3.6 Rezultatų interpretavimas ir apibendrinimas - Pakartotinio prisijungimo posistemė

Atlikus rezultatų analizę tolimesnis žingsnis yra rezultatų interpretavimas bei apibendrinimas. Gauti rezultatai buvo panaudoti pasitikėjimo elementų reitingavimui bei galimų scenarijų kūrimui. Kaip jau buvo minėta, elektroninio balsavimo sistemose susideda iš šešių pagrindinių etapų, tačiau siūlyme įterpiamas papildomas etapas – pakartotinis prisijungimas. Pav. 33 atvaizduota kaip šie etapai susiję tarpusavyje.

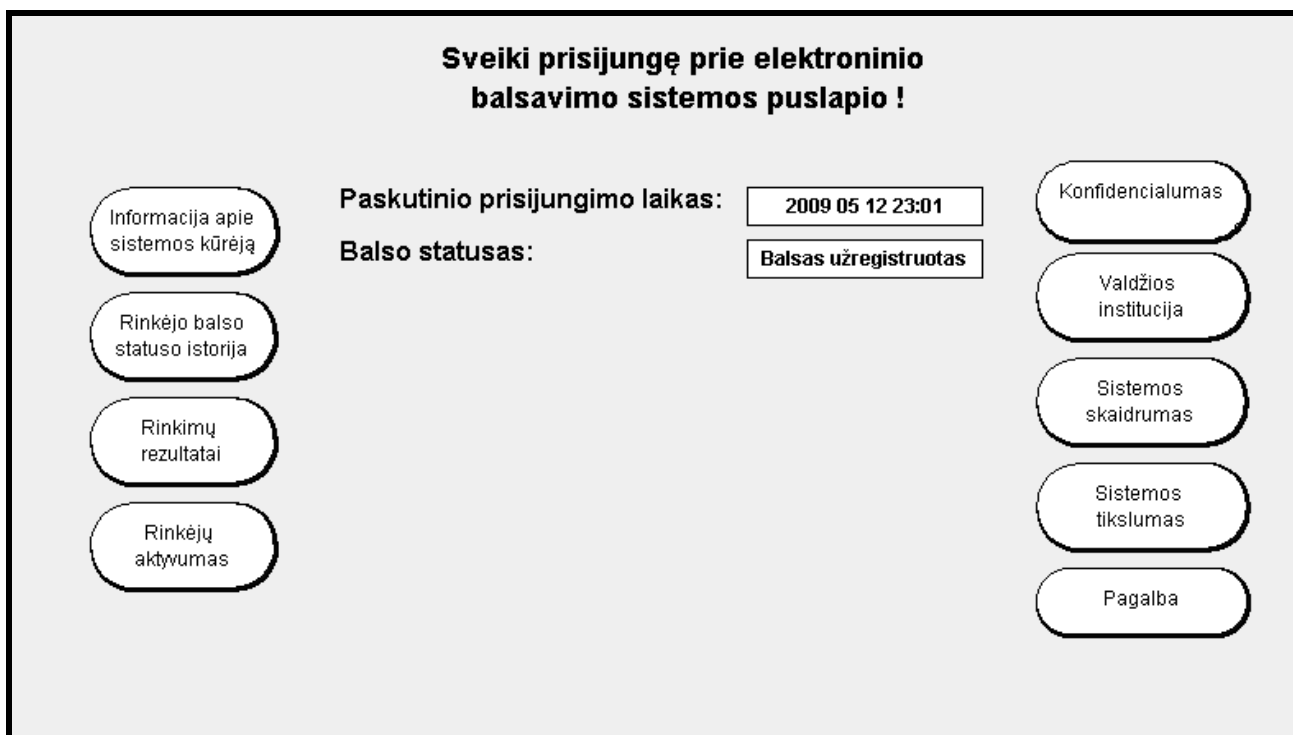


Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 60.

33 pav. Balsavimo etapai.

Pakartotiniam prisijungimui keliami reikalavimai, kad vyktų išsamus kiekvienoje balsavimo fazėje įvykusio veiksmo atvaizdavimas rinkėjui bei pasitikėjimo elementų akcentavimas atitinkamuose etapuose. Prisijungus prie sistemos pateikiama:

- Informacija apie sistemos kūrėją;
- Pagalbos galimybės;
- Balsavimo data bei laikas;
- Rinkėjo statusas el. balsavimo sistemoje;
- Rinkimų rezultatai;
- Rinkėjų aktyvumo statistika.

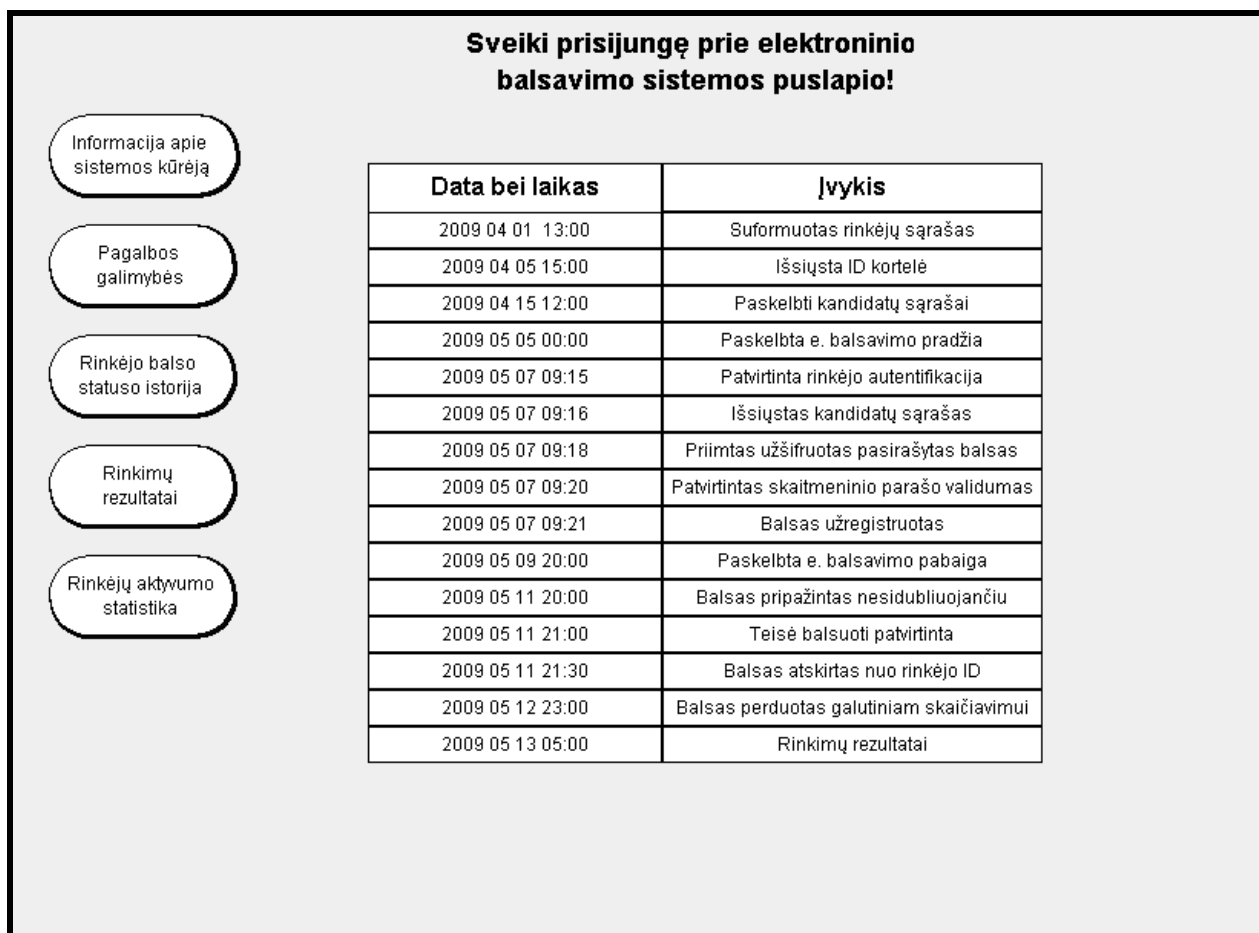


Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 61.

34 pav. Pakartotinio prisijungimo langas.

Informacija apie sistemos kūrėją – pateikiama išsami informacija apie sistemos kūrėją. Remiantis apibendrintu pasitikėjimą el. balsavimu kuriančiu modeliu vienas iš svarbiausių sistemai pasitikėjimą kuriančių veiksnių yra individualaus piliečio elgesio požymiai bei instituciniai požymiai. T.y. polinkis į el. balsavimą, susipažinimas su sistema, organizacijos reputacija, autoritetas bei kompetencija.

Rinkėjo balso statuso istorija - kaip atvaizduota 35 pav., rinkėjas pereina skirtingas fazes. Pakartotinio prisijungimo metu jis gali stebėti savo veiksmų istoriją bei įsitikinti, kad jo balsas buvo užregistruotas galutiniame balsų skaičiavime.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 62.

35 pav. Rinkėjo balso statuso istorija

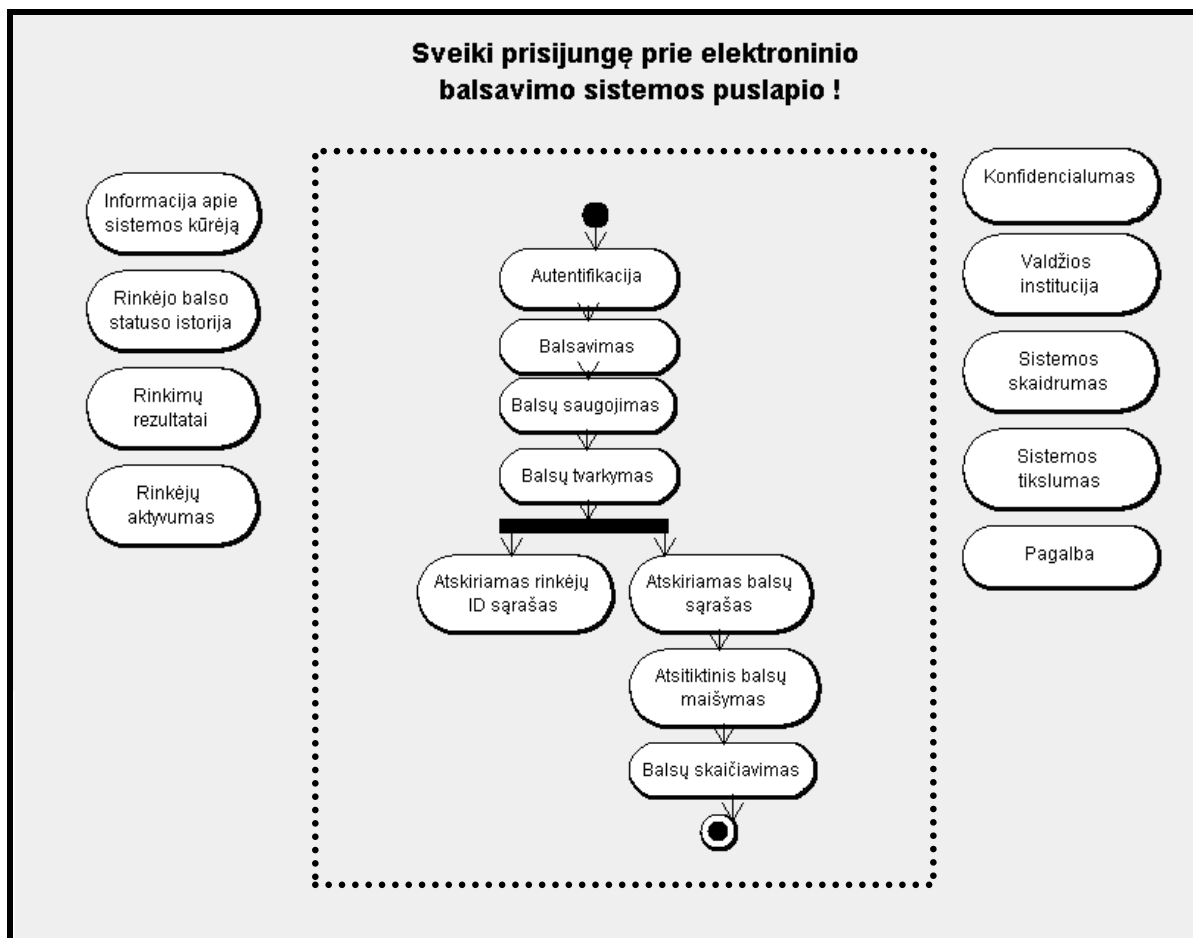
Rinkimų rezultatai – tai skiltis, kurioje skelbiami rinkimų rezultatai – preliminarūs bei galutiniai. Skelbiama informacija pagal apygardas, apskritis bei šalies mastu. Tai gali dar labiau sudominti rinkėją naudotis šia pakartotinio prisijungimo sistema bei suteikti pasitikėjimo kaip naujausios ir patikimos informacijos šaltiniu.

Rinkėjų aktyvumas – statistinė informacija apie balsavusius rinkėjus, koks aktyvumas pasiektas balsuojant internetu, balsuojant paštu bei įprastu būdu.

3.6.1 Rinkėjo konfidencialumas

Viena iš patikimiausių priemonių rinkėjo konfidencialumui užtikrinti yra atskirai saugoma rinkėjo asmeninė informacija bei jo balsas. Naudojant Estijos balsavimo sistemos prototipą, balsus saugantis serveris atskiria skaitmeninius parašus nuo balsų. Taip nelieka jokio ryšio tarp rinkėjo ir jo pasirinkimo. Be to balsus saugantis serveris atlieka atsitiktinį maišymą, tuo būdu negalima atkurti rinkėjų pasirinkimo, naudojant rinkėjų ID sąrašą. Tačiau sunkumas iškyla siekiant atvaizduoti šį faktorių vartotojui, kadangi skaitmeninių parašų nuo balsų atskyrimas vyksta po balsavimo, kuomet

virtotojas jau yra atsijungęs nuo sistemos. Tam gali būti panaudota pakartotinio prisijungimo posistemė arba trumpa schema balsavimo lange prieš balsuojant.

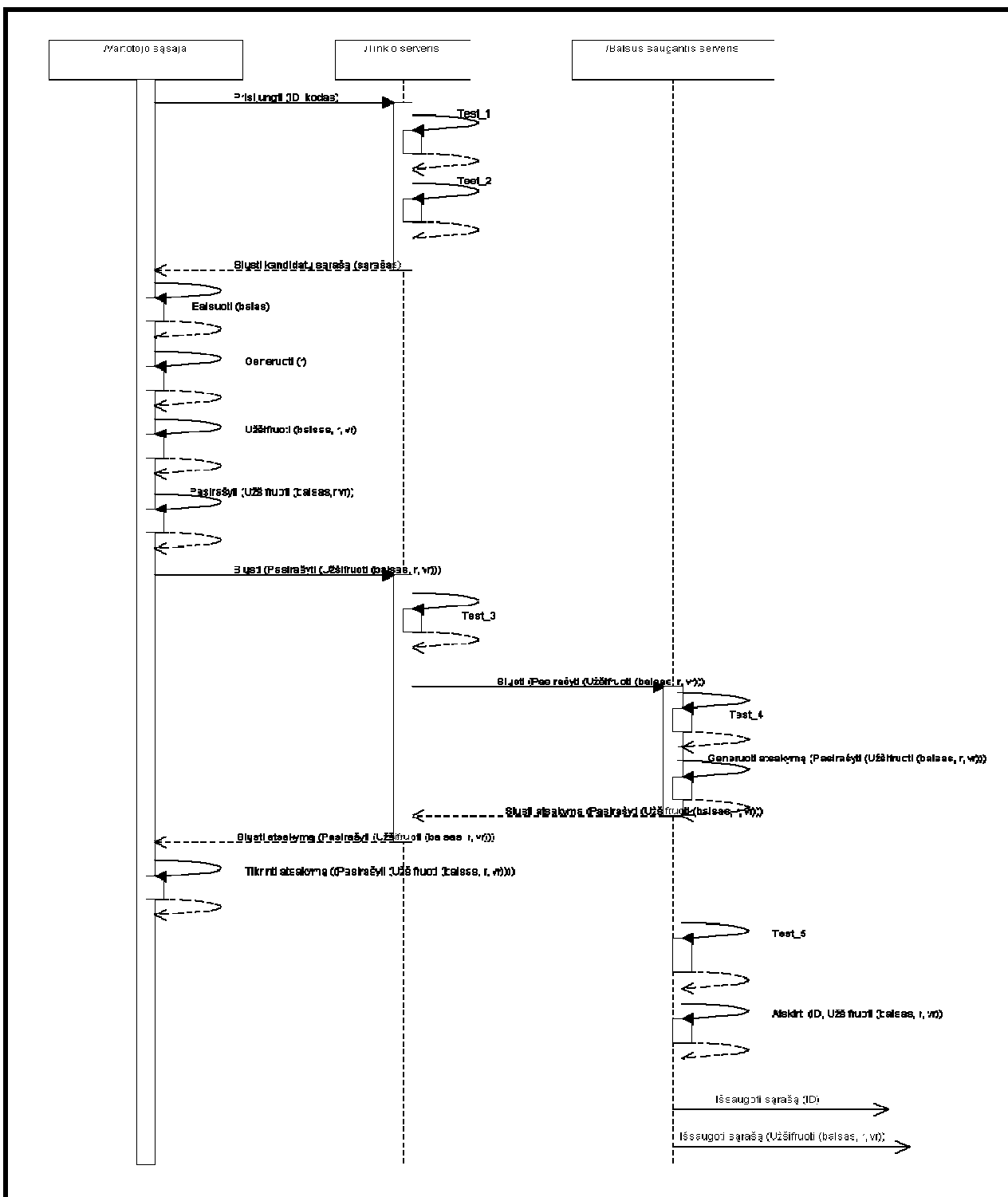


Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 63.

36 pav. Balsų nuo rinkėjų ID atskyrimas

36 pav. atvaizduoja darbą, kurį atlieka sistema, apdorodama ir valdydama balsus 37 pav. Vartotojas jungiasi ir autentifikuoja save. Test_1 bei Test_2 yra funkcijos tinklo serveryje, kurios tikrina ar vartotojas turi teisę balsuoti bei ar rinkėjas jau balsavo prieš anksčiau. Jei vartotojas turi teisę balsuoti, jam parodomas kandidatų sąrašas. Kandidatų sąrašė rinkėjas išsirenka kandidatą. Vartotojo sąsaja sugeneruoja atsitiktinį skaičių r bei užšifruoja su viešuoju raktu. Po to įveddamas PIN2 kodą rinkėjas pasirašo užšifruotą balsą patvirtindamas savo pasirinkimą. Šis užšifruotas bei pasirašytas balsas, r bei VR siunčiami į Tinklo serverį. Tinklo serveris patikrina ar asmuo, kuris autentifikavosi yra tas pats asmuo, kuris pasirašė balsą. Teigiamo atsakymo atveju, tinklo serveris persiunčia balsą, r bei VR į Balsus saugantį serverį. Balsus saugantis serveris su Test_4 patikrina SP validumą. Teigiamo atsakymo atveju generuoja atsakymą vartotojui. Po balsavimo laikotarpio pabaigos, Balsus saugantis serveris išima besidubliuojančius balsus, po to sudaromas balsų failas bei rinkėjų balsavusių el. balsavimo metu sąrašas (atskiriami balsai nuo ID). Balsų sąrašas

atsitiktinai maišomas siekiant konfidencialumo ir galimo balsų su ID sąrašu atkūrimo. Užšifruotų balsų failas įrašomas į laikmeną ir perduodamas į Balsus skaičiuojantį serverį.



Šaltinis: sukurta autoriaus pagal MAGI, T. (2007) Practical Security Analysis of E-voting Systems; KRIMMER, R. (2004) How Security problems Can Compromise Remote Internet Voting Systems.

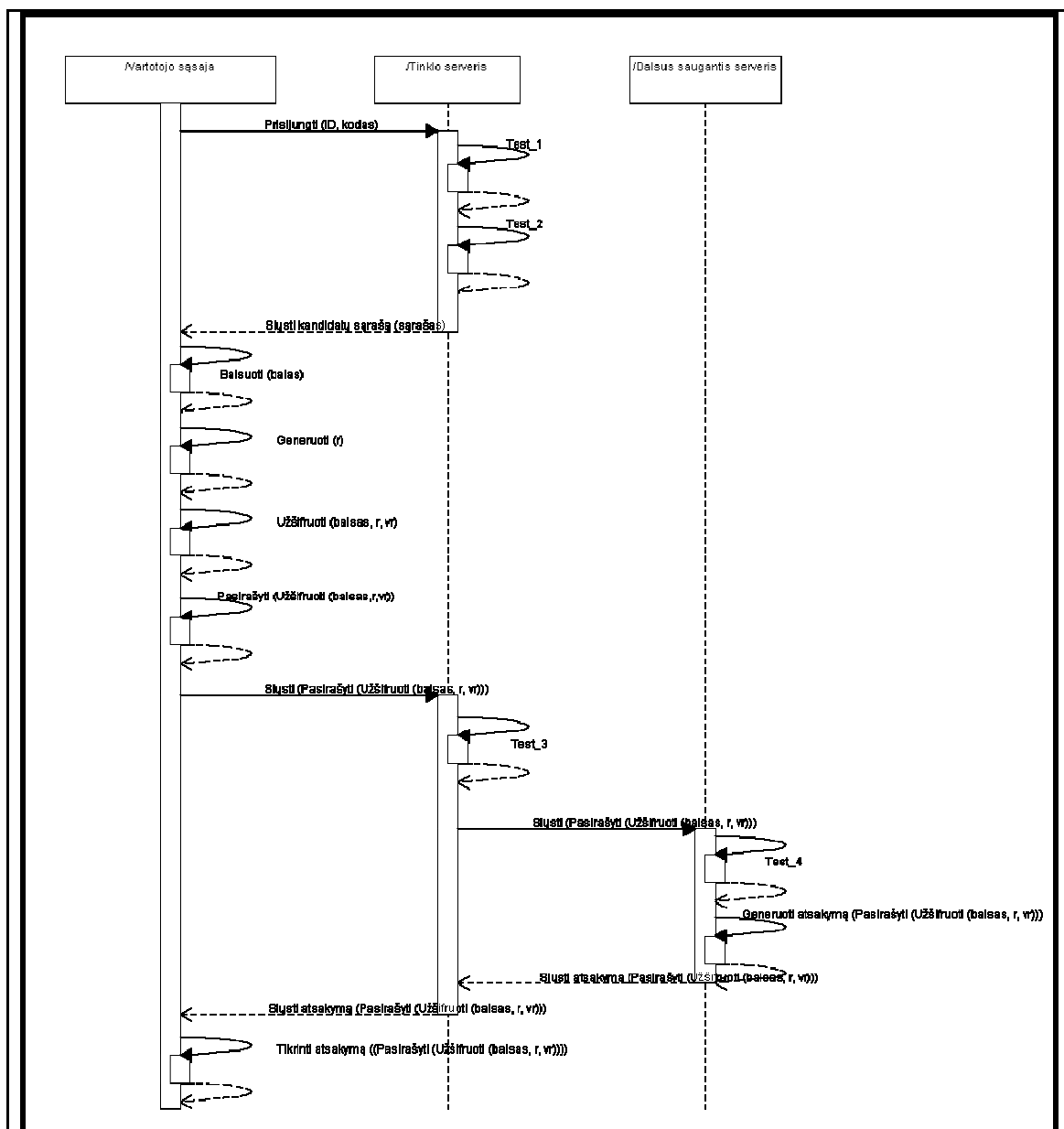
37 pav. Balsavimo procesas iki balsų atskyrimo.

3.6.1 Valdžios institucija

Atliekant teorinių pasitikėjimo el. valdžia modelių analizę buvo nustatyta, kad pasitikėjimas valdžios institucija tiesiogiai veikia pasitikėjimą el. valdžia bei tuo pačiu el. balsavimu. Organizacijos reputacija, reiškia, kad pilietis susieja savybes su antrine informacija gauta apie organizaciją. Jei valdžia vykdo savo pareigas ir atlieka paslaugas piliečiams tinkamai tikėtina, jog pilietis pasitikės el. balsavimo sistema. Remiantis Thomas (1998) topologija, pasitikėjimas valdžia yra kuriamas per tris veiksnius: charakteristikomis paremtu pasitikėjimu, procesu paremtu pasitikėjimu bei instituciniu pasitikėjimu (Thomas, C.W. (1998)). **Charakteristikomis paremtas pasitikėjimas:** sudėtinga manipuluoti asmeninėmis piliečių savybėmis. Patikimiausias būdas yra leisti piliečiams bendrauti su asmenimis turinčiais panašias savybes. Valdžios institucija turi pasirūpinti, kad asmuo atstovaujantis piliečiams, šiuo atveju rinkimų komisijos atsakingi asmenys, sistemos kūrėjai dalintųsi panašiomis asmeninėmis charakteristikomis bei taam tikrais būdais bendrautų su rinkėjais. **Procesu paremtas pasitikėjimas:** valdžios atstovų dalyvavimas visuomeniniame pasaulyje. Taip pat jų interaktyvumo lygis su piliečiais. Valdžios atstovų bendravimas su piliečiais, ieškojimas bendrų sąlyčio taškų problemoms spręsti, etiškumas. Sistema turi užtikrinti piliečiams galimybę išreikšti savo nuomonę bei gauti atgalinį ryšį. Tai gali būti atlikta per forumus ar per tiesioginio ryšio konferencijas. **Institucinis pasitikėjimas:** etikos normų taikymas bei laikymasis valdžios atstovų tarpe. Sukurti įstatymai, taisyklės ir draudimai bei nustatyti veikimo standartai ar įstatyminė išorinė peržiūra.

3.6.3 Sistemos skaidrumas

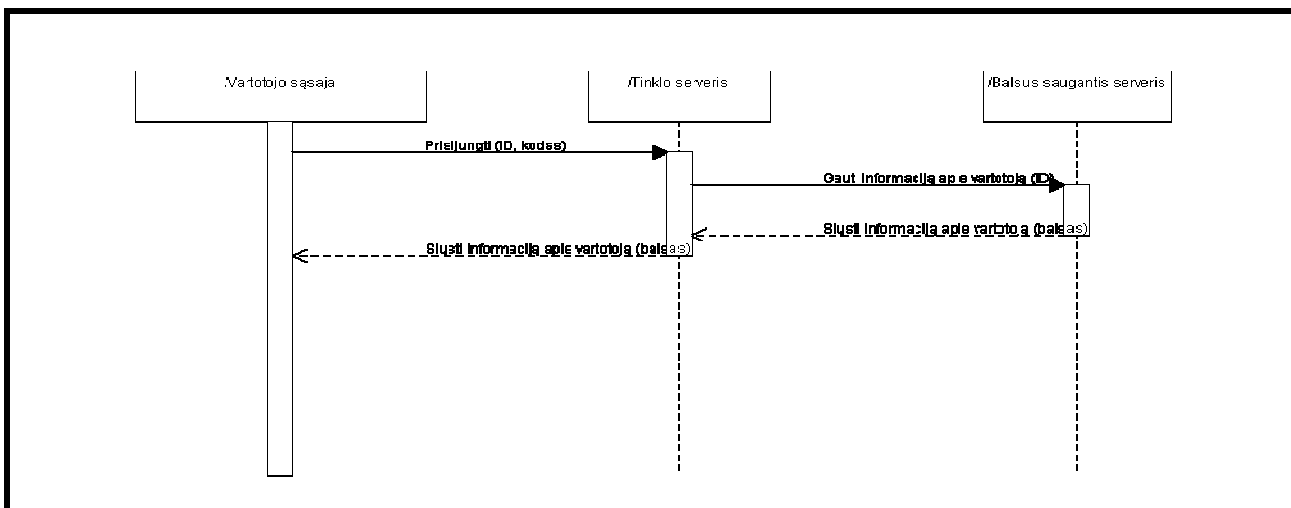
Rinkėjai privalo žinoti, jog jų balsai bus įskaičiuoti į galutinį rezultatą. Sistemoje realizuojamas atsiunčiant patvirtinimą apie balso užregistravimą bei sukuriant patogią informatyvią pakartotinio prisijungimo posistemę. Patvirtinimas turėtų būti parodytas po balso užregistravimo.



Šaltinis: sukurta autoriaus pagal MAGI, T. (2007) Practical Security Analysis of E-voting Systems; KRIMMER, R. (2004) How Security problems Can Compromise Remote Internet Voting Systems.

38 pav. Patvirtinimas apie balso užregistravimą.

Balsavimo pabaigoje patvirtinimo žinutė yra atvaizduojama ekrane, taip pat šis patvirtinimas gali būti atspausdintas. Atvaizduojamoje žinutėje parodoma laikas ir data rinkėjo registracijos. Rinkėjas gali pakartotinai prisijungti prie sistemos ir patikrinti ar jo balsas užregistruotas ar ne. Vartotojas turi pakartotinai įdėti savo ID kortelę ir suvesti PIN1 kodą. Pakartotinis prisijungimas atvaizduotas 36 pav.



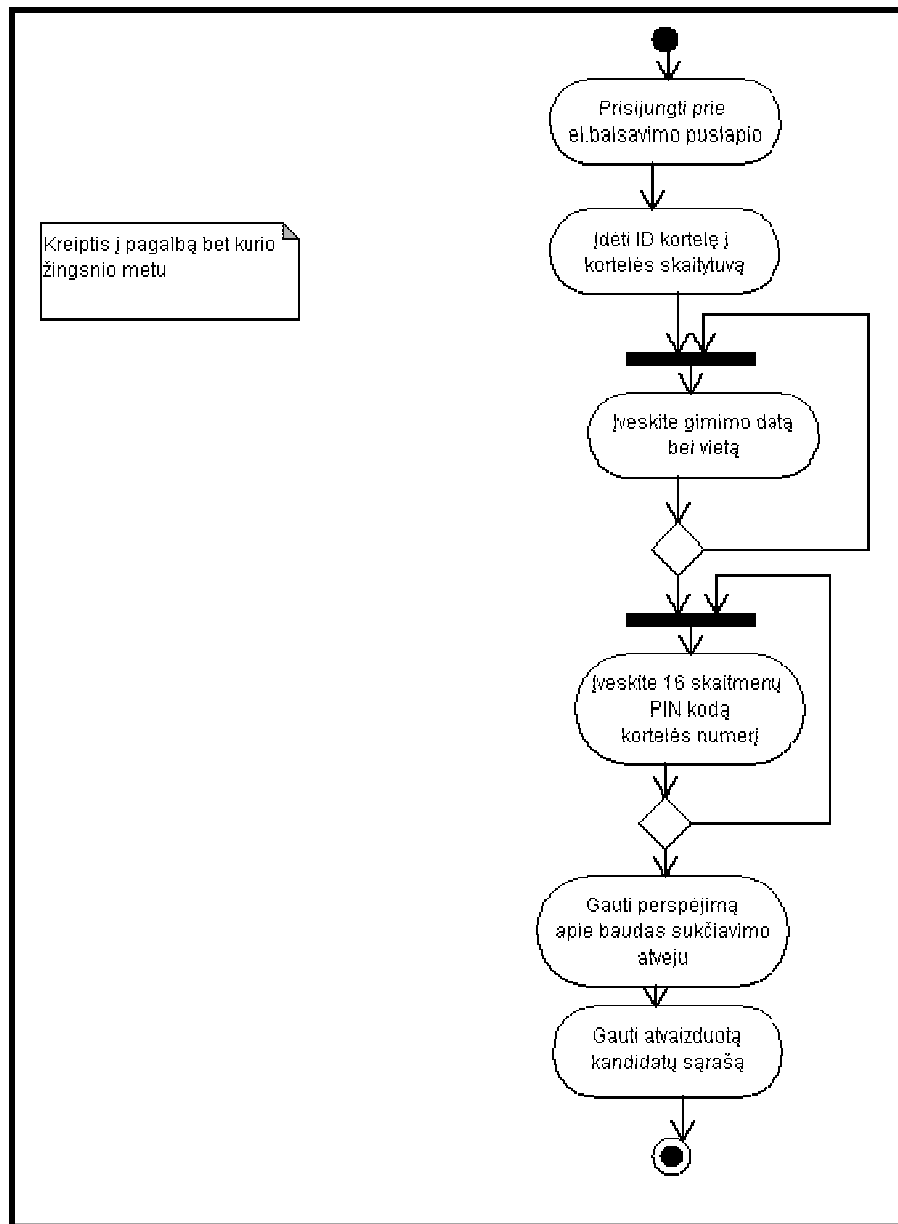
Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 67.

39 pav. Pakartotinis prisijungimas prie sistemos.

3.6.4 Sistemos tikslumas

Patikima autentifikacija, kuomet asmuo, dalyvaujantis rinkimuose identifikuojamas kaip asmuo, kuris jis skelbiasi esąs. Tik asmenys, turintys teisę balsuoti gali dalyvauti rinkimuose ir asmenys neturintys teisės balsuoti negali dalyvauti rinkimuose. Remiantis apklausa autentifikacijai labiausiai tinkama ID kortelė su skaitmeniniu parašu (71% respondentų). Kaip pavyzdys gali būti panaudota Estijos el. balsavimo sistemos projekto ID kortelė. Tačiau tuo atveju išauga el. balsavimo kaštai, nes šiai kortelei nuskaityti yra reikalingas kortelės nuskaitytuvas. Kitas būdas naudoti paprastą kortelę su prisijungimo vardu bei slaptažodžiu, šį būdą kaip tinkamą pripažino 63% apklaustųjų. Vis dėlto, tam kad pasiekti didesnę saugumą bei pasitikėjimą sistema turėtų būti naudojama ID kortelė su skaitmeniniu parašu bei du PIN kodai. Tam, kad rinkėjas būtų priimtas į balsavimo serverį, rinkėjas privalo įvesti teisingą savo gimimo vietą, datą bei balsavimo kortelės numerį (PIN1). 16 skaitmenų kodas negali būti atrastas atsitiktinai. Tikimybė, tokio pat skaičiaus atsitiktinai lygi vienai iš 5 milijardų. Po šio žingsnio rinkėjas gauna informaciją apie baudas apgavystės atveju bei elektroninį balsavimo biuletenį ekrane. Kortelė turėtų būti užblokuota po penkių nesėkmingų bandymų prisijungti. El. balsavimo laikas yra griežtai nustatytas prieš įprastinį balsavimą. Balsavimas internetu vyksta savaitę prieš balsavimo dieną ir sistema užsidaro šeštadienį vidurdienį. Balsavimas įprastu būdu vyksta nuo 10 ryto iki 6 vakaro sekmadienį. Automatinė kontrolė vartotojo sąsajoje atšaukia prisijungimą prie sistemos jei gimimo vietos bei datos, PIN1 bei PIN2 įvedami greičiau nei per 2 sec. Taip pat jei vartotojas neįveda bet kurio iš šių kodų per penkias minutes, jis yra atjungiamas nuo sistemos, kaip vartotojas bandantis atspėti slaptažodį. Tokiu būdu sistema būtų

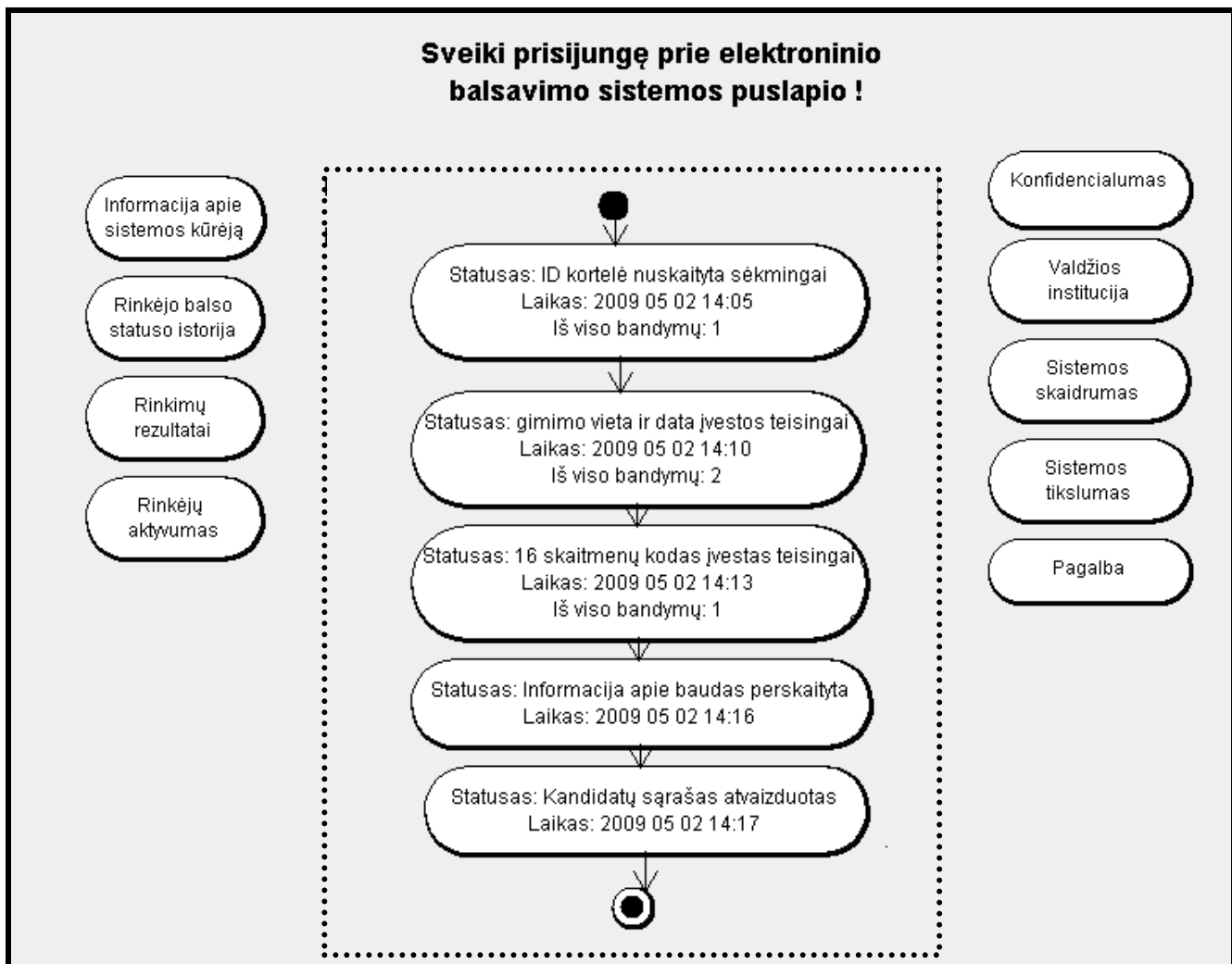
apsaugota nuo neturinčių teisės balsuoti asmenų prisijungimo. Pav. 37 pavaizduota diagrama, kuri parodo autentifikacijos veikimą.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 67.

40 pav. Autentifikacijos procesas el. balsavimo sistemoje

Tuo tarpu vartotojas turi gauti ir informaciją apie jo autentifikacijos procesą pakartotinio prisijungimo posistemėje (41 pav.).

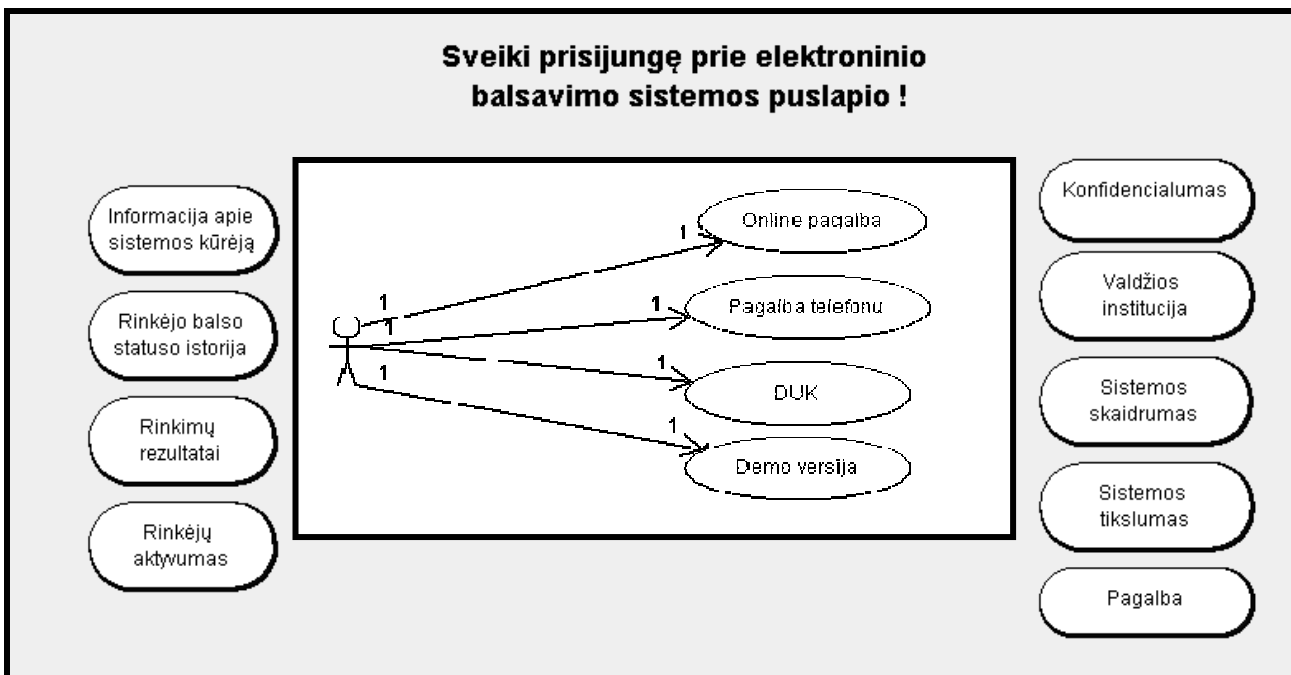


Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 69.

41 pav. Asmeninė autentifikacijos istorija.

3.6.5 Pagalba

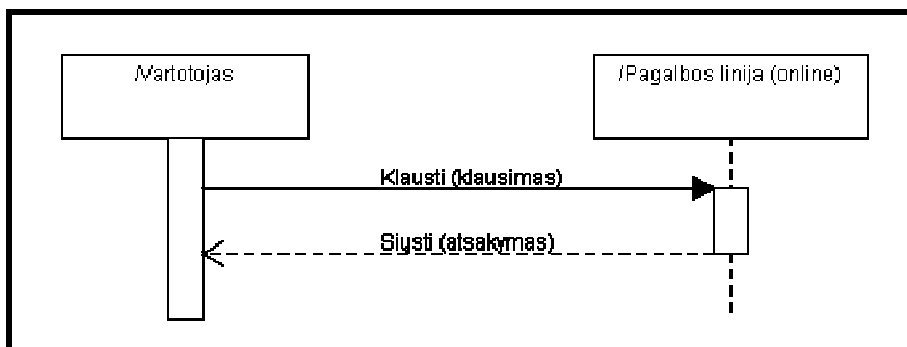
Vienas iš svarbių veiksnių veikiančių vartotojo pasitikėjimą sistema yra tinkama pagalba (70%). Tinkamiausia pagalba - online pagalba (77%), pagalba telefonu (65%) bei DUK (59%). Vartotojai įvardijo, kaip mažiausiai tinkamą pagalbą – programos demo versiją (50%).



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 70.

42 pav. Pagalbų rūšys.

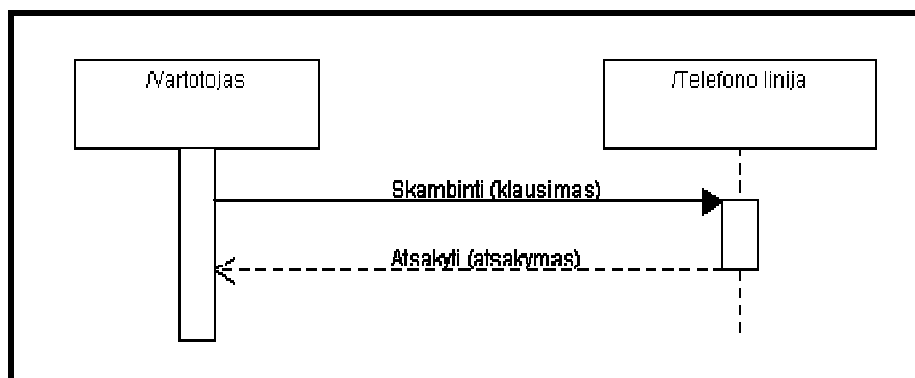
Online pagalba vyksta supaprastinta tvarka 43 pav., kai vartotojas kreipiasi su klausimu, o pagalbos linijos operatorius siunčia atsakymą.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 70.

43 pav. Online pagalba.

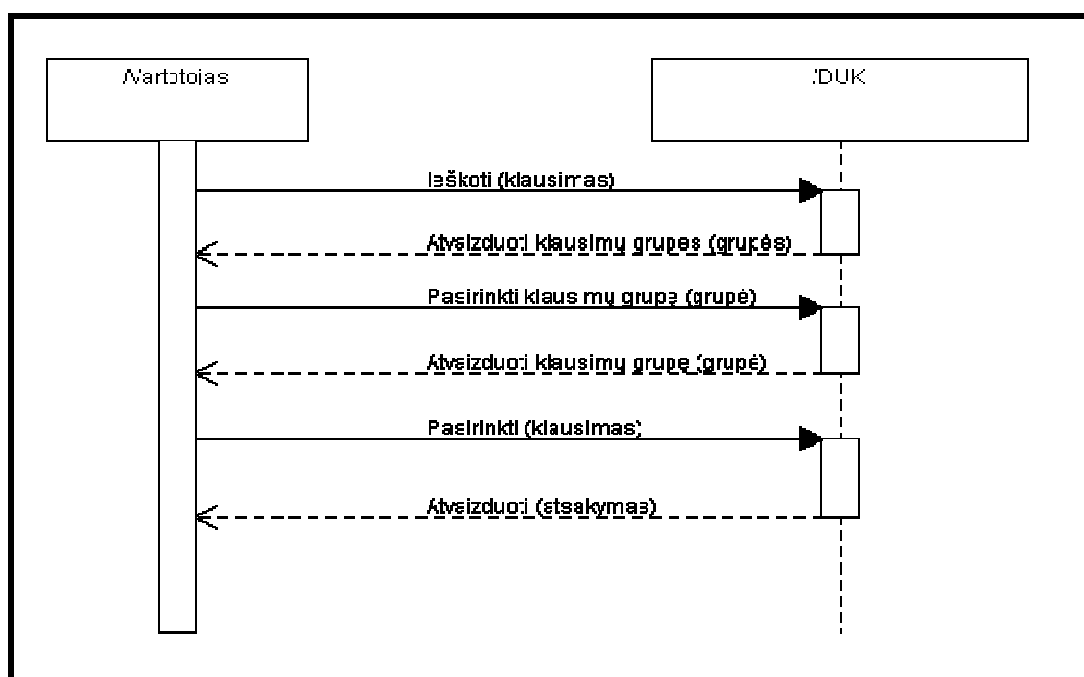
Pagalba telefonu 44 pav. vyksta panašiai kaip ir online pagalba, kai vartotojas skambina operatoriui su klausimu, o pagalbos linijos operatorius atsako į klausimą.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 71.

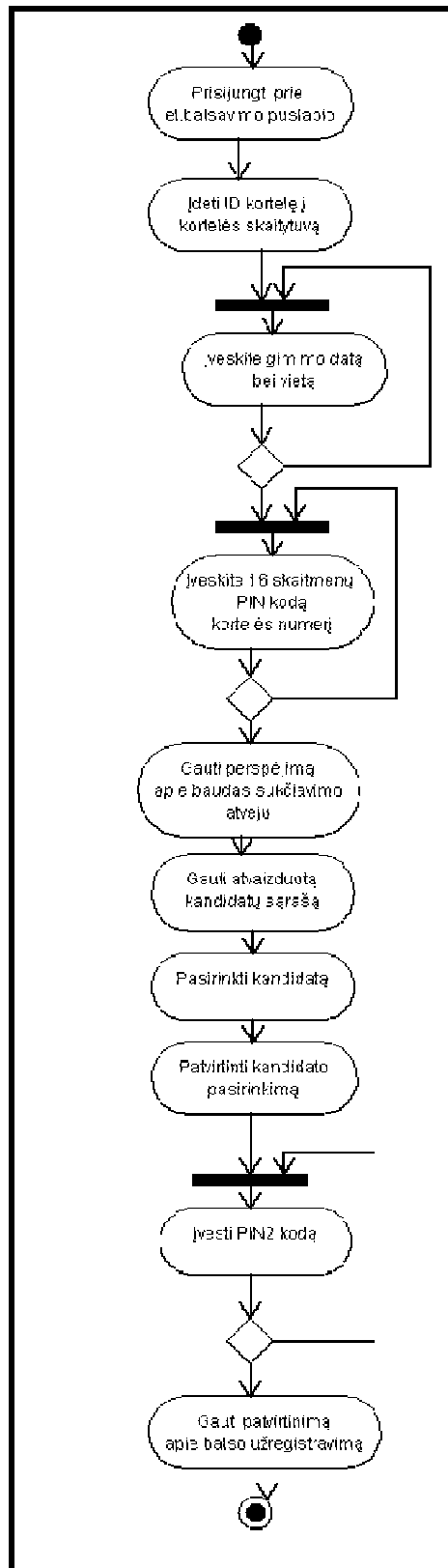
44 pav. Pagalba telefonu.

Siekiant paskatinti vartotojus naudotis DUK, reikalinga šią pagalbą sukurti kiek galima paprastesnę ir vartotojams patrauklesnę naudoti. Klausimai turėtų būti sugrupuoti į sričių grupes. Iš vartotojo sąsajos atvaizduotų klausimų grupių vartotojas turėtų išsirinkti tinkamą jam grupę, tuomet vartotojo sąsaja turėtų atvaizduoti visus klausimus priklausančius tai grupei ir vartotojas galėtų pasirinkti jam rūpimą klausimą. Pagalba naudojant DUK atvaizduota 45 pav.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 71.

45 pav. Pagalba naudojant DUK.



Šaltinis: ŠOLYTĖ, G. (2009) Pasitikėjimo elementų elektroninio balsavimo sistemose tyrimas, p. 72.

46 pav. Demo versija.

3.7 Eksperimentinio skyriaus išvados

Anketos klausimai buvo sudaryti, siekiant patikrinti pasitikėjimą el. balsavimo sistemomis kuriantį modelį ir siekiant išsiaiškinti, kurie pasiūlyti elementai yra svarbiausi, o kurie vartotojui įtakos nedaro. Nagrinėtose sistemose apžvelgti elementai naudojami skirtingai, buvo iširta, kurie elementai būtini vartotojo atžvilgiu, sekančiai vaizduojami pagal gauto tyrimo rezultatus sureitinguoti pasitikėjimo elementai, mažėjimo tvarka:

- 1) **(4) Rinkėjo konfidencialumas** svarbus (85%) apklaustųjų.
- 2) **(8) Pasitikėjimas valdžia** - 84% apklaustųjų įvardijo, kaip svarbų faktorių. 51% apklaustųjų naudojami valdžios paslaugomis, net 53% apklaustųjų mano, kad el. balsavimas reikalingas įdiegti jų šalyse. Be to, tinkamiausiu el. balsavimo sistemos kūrėju bei palaikytoju, respondentai laiko valdžios instituciją 61%.
- 3) **(2) Sistemos skaidrumas** išreikštas per patvirtinimą apie balso užregistravimą (83%). Be to priimtinausias būdas patvirtinti, kad balsas buvo užregistruotas yra rinkimų puslapis (66%).
- 4) **(1) Rinkimų tikslumas** – rinkėjo autentifikacija (82%). Autentifikacijai labiausiai tinkama ID kortelė su skaitmeniniu parašu (71%) bei prisijungimo vardas su slaptažodžiu (63%). Apklaustieji įvardijo, kad nutrinamų kodų kortelė bei e-bankininkystės sistema autentifikacijai netinkama.
- 5) **(7) Pagalba** svarbus (70%), tinkamiausia pagalba - online pagalba (77%), pagalba telefonu (65%) bei DUK (59%).
- 6) **(5) Sistemos saugumas** - informavimas, jog balsas užšifruotas kriptografiniu metodu (62%) ir sistema naudoja saugų ryšio kanalą perdavimui (63%).
- 7) **(6) Sistemos slaptumas** - kompetetingų rinkimų komisijos atstovų dalyvavimas balsų skaičiavime (56%).
- 8) **(9) Auditas** - sistemos auditas, svarbus elementas tik 44% apklaustųjų, - informavimas apie balsų perskaičiavimo galimybę 66% apklaustųjų.
- 9) **(3) Pakartotinis balsavimas** svarbus elementas 40% apklaustųjų.

Svarbiausias veiksnys apklaustiesiems yra rinkėjo konfidencialumas, po to pasitikėjimas valdžia, trečiasis faktorius - patvirtinimas apie balso užregistravimą. Ketvirtas elementas - rinkėjo autentifikacija, penktas – pagalba, šeštasis – sistemos saugumas. Buvo nustatyta, kad rinkėjams nėra svarbu sistemos auditavimas, kompetetingų rinkimų komisijos atstovų dalyvavimas balsų skaičiavime bei pakartotinio balsavimo galimybė.

Taip pat atlikus šią dalį buvo patobulintas pasitikėjimą el. balsavimo sistemose kuriantis modelis. Buvo nubraižyti sistemos veikimo scenarijai su elementais, kurie rinkėjams yra svarbūs kuriant pasitikėjimą el. balsavimo sistema. Didelis dėmesys buvo skirtas pakartotinio prisijungimo posistemei, kuri turėtų padidinti pasitikėjimą el. balsavimo sistema. Buvo atvaizduota diagramų bei jų aprašų pagalba būdai pasitikėjimą kuriančių elementų atvaizdavimui.

IŠVADOS

1. Atlikus darbą buvo išanalizuoti teoriniai pasitikėjimo el. valdžia modeliai. Faktoriai lemiantys pasitikėjimą el. valdžia buvo suskirstyti į dvi grupes: veikiančius prieš sąveiką su sistema ir sąveikos metu. Apibendrintas pasitikėjimo el. valdžia teorinis modelis susideda iš piliečio, el. valdžios sistemos ir technologijų bei trečiosios šalies. Prieš sąveiką veikiantys veiksniai tai - individualaus piliečio elgesio požymiai, instituciniai bei technologiniai veiksniai. Sąveikos metu veikia paslaugos, tranzakcijos išpildymo bei informacijos atributai. Individualaus piliečio elgesio požymiai apibrėžiami kaip asmens normos, demografija, bendros intencijos pasitikėjimui ir el. paslaugų naudojimas, kitų asmenų nuomonė bei patirtis, kultūra bei tradicijos. Instituciniai veiksniai - valdžios institucija, jos reputacija, patikimumas, įstatyminiai reikalavimai bei kompetencija veikia rinkėjo pasitikėjimą. Technologiniai faktoriai lengviausiai paveikiami iš sistemos kūrėjų pusės. Svarbiausi šios grupės aspektai yra perdavimo kokybė, sąsajos dizainas ir sudėtis, saugumas, skaitmeninis sertifikatas, viešojo rakto infrastruktūra, vientisumas, kompetencija ir nuspėjamumas, privatumas, tranzakcijos nuoseklumas, prieinamumas ir konfidencialumas. Sąveikos su sistema metu veikiantys paslaugos požymiai patikimumas, pritaikomumas individualiam vartotojui, prieinamumas ir kokybė yra taip pat svarbūs el. valdžios paslaugų vartotojui. Be to tranzakcija turi būti skaidri, tiksli bei kokybiška, turi vykti aptarnavimas po tranzakcijos įvykdymo. Paskutinioji veiksnių grupė siekia užtikrinti pasitikėjimą per informacijos savybes, nustatydama, kad informacija turi būti tiksli, išbaigta, nešališka, patikima, naudinga ir kokybiška.

2. Visuotinai el. balsavimo sistemos susideda iš šešių pagrindinių fazių: rinkėjo registracijos, autentifikacijos, balsavimo ir balsų saugojimo, balsų valdymo, balsų skaičiavimo bei audito. Išnagrinėjus sistemas paaiškėjo pagrindiniai skirtumai tarp jų realizacijos. Estijos el. balsavimo sistema naudoja ID korteles su skaitmeniniu parašu, o Šveicarijos realizuota el. balsavimo sistemoje panaudota balsavimo kortelės su nutrinamu sluoksniu. Autentifikacija vykdoma jau minėtų kortelių pagalba, tačiau įvedant skirtingus kodus, be to Estijos el. balsavimo sistema pasižymi galimybe balsuoti pakartotinai. Balsavimas bei balsų saugojimas panašūs tuo, kad šiose fazėse siekiama išsaugoti rinkėjo privatumą bei rinkimų saugumą. Be to Šveicarijos el. balsavimo sistemoje realizuotas puslapis, kuriame vartotojas gali patikrinti ar jo balsas pateko į galutinę balsadėžę. Balsų valdyme svarbus yra balsų perdavimas – Estijos el. balsavimo sistemoje naudojamas dvigubas šifravimas, o Šveicarijos sistemoje šifravimas bei balso konvertavimas į grafinį vaizdą. Rinkėjams svarbus aspektas, kad abi sistemos siekia išsaugoti rinkėjo privatumą ir prieš balsų skaičiavimo fazę atskiria rinkėjų sąrašus nuo jų balsų. Balsų skaičiavimas vykdomas nuo

tinklo atskirtame serveryje, bei balsavimo rezultatai saugomi atitininkamą laikotarpį abiejose nagrinėtose sistemose. Paskutinė el. balsavimo fazė, kuri svarbi vartotojui kaip sistemos patikimo veikimo garantas yra auditas. Abi sistemos naudoja log failuose išsaugotą informaciją, auditui atlikti. Be to, Šveicarijos el. balsavimo sistema naudoja išorinį auditą, kai įtraukiami politinių partijų kontrolieriai, kurie testuoja sistemą.

Darbe buvo apibendrintos Šveicarijos bei Estijos el. balsavimo sistemos bei atlikta jų analizė, to pasekoje buvo pasiūlytas pasitikėjimą el. balsavimo sistemomis kuriantis modelis. Jis apima devynis pagrindinius elementus. Pasitikėjimą kuriantys elementai: (1) **Sistemos tikslumas** – patikima autentifikacija, asmuo, dalyvaujantis rinkimuose identifikuojamas kaip asmuo, kuris jis skelbiasi esąs. Nagrinėtose sistemose vykdomas skirtingai, tačiau saugiausias iš jų ID kortelės su skaitmeniniu parašu panaudojimas, bei dvigubo kodo apsauga, naudojant PIN1 – gimimo datą bei vietą, o PIN2 – 16 skaitmenų kodą atspausdintą ant kortelės. (2) **Sistemos skaidrumas** - rinkėjai privalo žinoti, jog jų balsai bus įskaičiuoti į galutinį rezultatą. Sistemoje realizuojamas atsiunčiant pranešimą bei sukuriant informatyvią pakartotinio prisijungimo posistemę. (3) **Pakartotinis balsavimas** – realizuotas pakartotinis balsavimas rinkėjui pakeitus pasirinkimą, tačiau užtikrinamas prieš tai buvusio balso išėmimas iš sistemos ir rinkėjo balsas gali būti įskaičiuotas į galutinį balsų skaičiavimą tik vieną kartą. (4) **Rinkėjų konfidencialumas** – balsus skaičiuojančiame serveryje atskirai saugoma rinkėjo asmeninė informacija bei jo balsas. Be to atskirtų balsų bei rinkėjų ID sąrašai nuolatos maišomi siekiant atsitiktinio generavimo bei siekiant nutraukti bet kokius mėginimus susieti šiuos du sąrašus. 5) **Sistemos saugumas** - perdavimo kanalas tarp rinkėjo ir serverio turi būti saugus, rinkėjai turi būti tikri, kad jų balsai nusiųsti į oficialų serverį ir, kad balsai apsaugoti nuo trečiosios šalies priėjimo. Šifravimui naudojami kriptografiniai metodai bei saugaus ryšio kanalo panaudojimas balso perdavimui. (6) **Sistemos slaptumas** - rinkėjų pasirinkimas nebus atskleistas jokiais aplinkybėmis. Realizuotas panaudojant jau minėtas saugumo priemones bei dešifravimui reikalingą privatų raktą padalinus tarp įgaliotų rinkimų komisijos atstovų. (7) **Pakankamos pagalbos** rinkėjams užtikrinimas: pagalba išdėstyta patogiai lange, į ją kreipiamasi bet kuriuo metu, be to, rinkėjas gali grįžti atgal visame balsavimo procese. (8) **Pasitikėjimas valdžia** - išsami informacija apie sistemos kūrėją, atvaizduojama vartotojo sąsajoje prieš autentifikaciją taip pat pakartotinio prisijungimo posistemėje. (9) **Auditas** - informacija, kad sistema audituojama viso proceso metu. Reikalinga dėl sistemos patikimumo.

3. Siekiant patikrinti modelio veiksmingumą buvo sudaryti anketos klausimai. Nagrinėtose sistemose apžvelgti elementai naudojami skirtingai, buvo ištirta, kurie elementai būtini vartotojo pasitikėjimui didinti. Gauti rezultatai parodė, kad svarbiausias veiksnys apklaustiesiems yra rinkėjo konfidencialumas 85% apklaustųjų., po to pasitikėjimas valdžia 84% apklaustųjų,

trečiasis faktorius - patvirtinimas apie balso užregistravimą išreikštas per patvirtinimą apie balso užregistravimą (83%). Ketvirtas elementas - rinkėjo autentifikacija 82% apklaustųjų, penktas – pagalba (70%), šeštasis – sistemos saugumas: informavimas, jog balsas užšifruotas kriptografiniu metodu (62%) ir sistema naudoja saugų ryšio kanalą perdavimui (63%). Buvo nustatyta, kad rinkėjams nėra svarbu sistemos auditavimas (44%), kompetetingų rinkimų komisijos atstovų dalyvavimas balsų skaičiavime (56%) bei pakartotinio balsavimo galimybė 40% apklaustųjų.

4. Atlikus darbą siūloma stiprinti nustatytų pasitikėjimo elementų diegimą el. balsavimo sistemose. Taip pat siūloma remiantis darbu didesnę dėmesį skirti pakartotinio prisijungimo posistemei, kuri turėtų padidinti pasitikėjimą el. balsavimo sistema. Ši posistemė turi būti kaip papildomas ir svarbus pasitikėjimą kuriantis elementas. Joje taip pat turi būti atvaizduojami vartotojui svarbūs jau minėti pasitikėjimo elementai.

Literatūra

Mokslinės literatūros sąrašas

1. BRYMAN, A.; BELL, E. (2007) Business research methods second edition. Oxford University Press Inc., New York. 40-41 p. ISBN 978-0-19-928498-6.
2. DAVID, J.; RUBIN, A.D.; BARBARA, S.; WAGNER, D. (2004) A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE) [interaktyvus]. [žiūrėta 2008 m. sausio 14d.]. Prieiga per internetą: <<http://servesecurityreport.org/paper.pdf>>.
3. JOHNS, J.L. (1996) A concept analysis of trust, Journal of Advanced Nursing volume 24, pp. 76–83.
4. KIM, D.J.; SONG, Y. I.; BRAYNOV, S.B.; RAO, H.R. (2005) A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/practitioner perspectives. Decision Support Systems volume 40, pp. 143-165.
5. KRIMMER, R. (2004) How Security problems Can Compromise Remote Internet Voting Systems [interaktyvus]. Aachen: Institute of Business Information Systems RWTH, Aachen University, [žiūrėta 2008 m. gegužės 14d.]. Prieiga per internetą: <http://www.e-voting.cc/static/evoting/files/schryen_p121-131.pdf>.
6. MAGI, T. (2007) Practical Security Analysis of E-voting Systems [interaktyvus]. Talinas: University of Technology, Department of Informatics, [žiūrėta 2008 m. balandžio 14d.]. Prieiga per internetą: <<http://triinu.net/e-voting/master%20thesis%20e-voting%20security.pdf>> .
7. McKNIGHT, D.H.; CHOUDHURY, V.; KACMAR, C. 2002. “The Impact of Initial Consumer Trust on Intentions to Transact with Web Sites: A Trust Building Mode”. Journal of Strategic Information Systems, 11: 297 – 323.
8. NAVEED, Z. Ch.; PILKJAER, A. (2007) E-voting in Pakistan [interaktyvus]. Pakistanas: Lulea Technologijos universitetas, [žiūrėta 2007 m. lapkričio 18d.]. Prieiga per internetą: <<http://epubl.ltu.se/1653-0187/2007/015/LTU-PB-EX-07015-SE.pdf>>.
9. NEUMANN, P.G. (1993) Security Criteria for Electronic Voting [interaktyvus]. JAV: Computer Science Laboratory SRI International, [žiūrėta 2008 m. balandžio 14d.]. Prieiga per internetą: <<http://www.csl.sri.com/users/neumann/ncs93.html>>.
10. PARENT, M.; VANDEBEEK, C.A.; GEMINO, A.C. (2005) Building citizen trust through e-government. Government information Quarterly volume 22, pp. 720-736.
11. RAMONAITĖ, A. (2008) Elektroninio balsavimo galimybių studija. [interaktyvus]. Vilnius: E-demokratijos tyrimų grupė, [žiūrėta 2008 m. sausio 17 d.]. Prieiga per internetą: <http://www.e-demokratija.lt/public_files/file_1200397814.pdf>.
12. SUNDGREN, A. (2005) What is a public information system? International Journal of Public Information Systems, volume 2005:1, pp. 81-99.
13. ŠARKIŪNAITĖ, D.; KRIKŠČIŪNIENĖ, D.; SIMUTIS, R. (2007) Magistro baigiamojo darbo rengimo tvarka. Kaunas. 15-16 p. ISBN 978-9955-33-011-0.
14. ŠOLYTE, G. (2009) Pasitikėjimo elementų el. balsavimo sistemose tyrimas. Pranešimas konferencijoje: IT 2009. Kaunas, 2009 m. gegužės 04 d.

15. TASSABEHJI, R.; ELLIMAN, T. (2006) Generating citizen trust in e-Government using a trust verification agent: a research note. European and Mediterranean Conference on Information Systems (EMCIS).
16. THOMAS, C.W. (1998) Maintaining and restoring public trust in government agencies and their employees. *Administration and Society* volume 30, no. 2, pp. 166-193.
17. TEO, T.S.H.; SRIVASTAVA, S.C.; JIANG, L. (2008). Trust and Electronic Government Success: An Empirical Study. *Journal of Management Information Systems* volume 25, no. 3, pp. 99-131.

Informacijos šaltinių sąrašas

18. BORRAS, J. (2007) Election Markup Language (EML) Version 5.0 [interaktyvus]. OASIS [žiūrėta 2008 m. gruodžio 17 d.]. Prieiga per internetą: <<http://docs.oasis-open.org/election/eml/v5.0/os/EML-Process-Data-Requirements-v5.0.pdf>>.
19. Capgemini. (2007) The User Challenge Benchmarking The Supply Of Online Public Services, 7th Measurement [interaktyvus]. Diegem (Belgium): Capgemini Belgium NV/SA, [žiūrėta 2008 m. gegužės 16d.]. Prieiga per internetą: <http://ec.europa.eu/information_society/europe/i2010/docs/benchmarking/egov_benchmark_2007.pdf>.
20. eGovernment News. (2004) EU: E-voting systems must be based on open standards, says Council of Europe [interaktyvus]. European Communities 2004 [žiūrėta 2008 m. lapkričio 17 d.]. Prieiga per internetą: <<http://www.epractice.eu/document/1125>>.
21. EPP, M. (2007) Internet voting system [interaktyvus]. Talinas: Estonian National Electoral Committee, [žiūrėta 2008 m. birželio 2 d.]. Prieiga per internetą: <<http://www.vvk.ee/english/epp.ppt>>.
22. Federal Office of Communications OFCOM. (2007) [Electronic voting](#) [interaktyvus]. Šveicarijos konfederacija: Federal Office of Communications, [žiūrėta 2008 m. gegužės 17 d.]. Prieiga per internetą: <<http://www.bakom.ch/themen/infosociety/01691/01706/index.html?lang=en>>.
23. DAMBAUSKAS, E. (2007) Analitinė studija: Dėl LR Seimo nutarimo „Dėl balsavimo internetu rinkimuose ir referendumuose koncepcijos patvirtinimo“ [interaktyvus]. Vilnius: Viešojo įstaiga Demokratinės politikos institutas (DPI), [žiūrėta 2007 m. gruodžio 25 d.]. Prieiga per internetą: <<http://www.dpi.lt/index.php?id=336>>.
24. KAČINSKIENĖ, A. (2007) Elektroninės valdžios plėtra Lietuvoje [interaktyvus]. Vilnius: Vidaus reikalų ministerija, [žiūrėta 2007 m. lapkričio 15d.]. Prieiga per internetą: <http://www.klaipeda.aps.lt/stotisFiles/uploadedAttachments/3_Kacinskiene.pdf>
25. KITCAT, J. (2007) Dutch voting computers decertified [interaktyvus]. Amsterdam: "Wij vertrouwen stemcomputers niet", [žiūrėta 2008 m. gegužės 18d.]. Prieiga per internetą: <<http://www.wijvertrouwenstemcomputersniet.nl/English>>.
26. Lietuvos Respublikos Seimas. (2006) Balsavimo internetu rinkimuose ir referendumuose koncepcija [interaktyvus]. Vilnius: Lietuvos Respublikos Seimas, [žiūrėta 2007m. gruodžio 19d.]. Prieiga per internetą: <<http://www3.lrs.lt/docs2/HUJQOGCB.DOC>>.
27. Lietuvos Respublikos Vyriausybė. (2006) Dėl Lietuvos Respublikos Vyriausybės 2003 m. lapkričio 25 d. Nutarimo nr. 1468 „Dėl Elektroninės valdžios koncepcijos įgyvendinimo priemonių plano patvirtinimo“ pakeitimo [interaktyvus]. Vilnius: Lietuvos Respublikos

- vyriausybė, [žiūrėta 2008 m. gegužės 12 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc?p_id=273105>.
28. State Chancellery. (2007) State Council's Report to the Grand Council on the Geneva electronic voting project [interaktyvus]. Republic and Canton of Geneva: State Chancellery, [žiūrėta 2008 m. gegužės 17 d.]. Prieiga per internetą: <http://www.ge.ch/evoting/english/doc/rapports/EN_RD_639_and_Annex.pdf>.
 29. The National Election Committee. (2005) E-voting system overview [interaktyvus]. Talinas: The National Election Committee, [žiūrėta 2008 m. Gegužės 4 d.]. Prieiga per internetą: <<http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf>>
 30. VAIGAUSKAS, Z. (2006) Lietuvos Respublikos Seimui Lietuvos Respublikos Vyriausios rinkimų komisijos pirmininko ataskaita už 2005 metus [interaktyvus]. Vilnius: Vyriausiosios rinkimų komisija, [žiūrėta 2008 m. gegužės 15d.]. Prieiga per internetą: <<http://www3.lrs.lt/docs2/REGOBIUT.DOC> >
 31. Vyriausioji rinkimų komisija. (2007a) Elektroninio balsavimo sistemos kūrimo darbai įgyja pagreitį [interaktyvus]. Vilnius: Vyriausioji rinkimų komisija, [žiūrėta 2008 m. gegužės 16d.]. Prieiga per internetą: <<http://www.vrk.lt/lt/naujienos/igyja-pagreiti.html>>
 32. Vyriausioji rinkimų komisija. (2007b) Sėkmingai tęsiami internetinio balsavimo sistemos kūrimo darbai [interaktyvus]. Vilnius: Vyriausioji rinkimų komisija, [žiūrėta 2008 m. birželio 17 d.]. Prieiga per internetą: <<http://www.vrk.lt/lt/naujienos/sekmingai-tesiami-internetinio-balsavimo-sistemos-kurimo-darbai.html>>

PRIEDAI

1 PRIEDAS

Anketa (angliška versija)

Dear respondent, I am student in Vilnius University, Faculty of Humanities in Kaunas. For my master thesis, I am doing research - **The research of trust elements in e-voting systems.**

Decreasing number of voters in elections, trigger us to find the ways how to facilitate voting procedure. The goal of this research is to find and understand factors, which determine trust of these systems among voters. Secondly, create scenarious which would improve e-voting sytem.

We ensure that your personal data will be not published and will be confidential.

We kindly ask to answer the questions of this questionnaire. All questionnaire will take not more than 10 min.

Please check only one possible answer.

1. What is your gender?

- Female
- Male

2. What is your age?

- Under 20
- 21-25
- 26-35
- 36-45
- 46-55
- 56-65
- More than 65

3. Where is your place of residence?

- Denmark
- Germany
- Lithuania
- Poland
- France
- Italy
- Other _____

4. What is your level of education?

- High School
- College
- University degree
- Master degree
- Other _____

5. What is the level of your computer use experience?

- None
- Average
- Advanced
- Expert

6. Do you use E-Government services?

- Yes
- No

7. If you answered yes, what kind of services provided by E-Government do you use?

- None
- Getting information
- Downloading forms and materials
- Paying taxes
- Issuing passport/ driving license
- Registering car
- Paying bills
- Voting
- Other _____

8. What way of voting is most suitable for you?

- Paper-based voting
- Internet voting
- Voting by post
- Other _____

9. Do you think there is a need of implementing e-voting system in your country?

- Yes
- No

10. If you answered yes, please choose factors (multiple choice) why you think there is a need of implementing e-voting system in your country?

- Staff on pooling booths can influence voting results
- Time to calculate voting results is too long
- Government can affect results of the voting by manipulating them
- Decreased percentage of people participating in elections
- Citizens abroad do not go to elections

11. Who should develop e-voting systems?

- Local company
- Government bodies
- Foreign company

12. Do you think, you could trust on e-voting systems?

- Yes
- No

13. Please evaluate the importance of factors affecting your trust in e-voting systems

	Very important	Important	Neither	Not important	Absolutely not important	Don't know
• Authentication	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Systems visibility	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Repeatable voting	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Voters confidentiality	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Help service	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• E-bank system use in e-voting system	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Trust in government institutions and elections	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

14. Do you trust your country government and elections system?

Yes, I trust fully	Yes, I trust	Neither	No, I do not trust	No, I do not trust at all	I do not have opinion
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

15. As a voter please evaluate the possible ways of authentication?

	Very suitable	Suitable	Neither	Not suitable	Absolutely not suitable	Don't know
• Login and password	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Scratch codes	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Digital signature	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Biometrical access	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• E-banking system	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Other _____	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

16. Do you as a voter need the proof of your vote registration to trust e-voting system more?

- Yes
- No

17. If you answered yes, please specify which tools are the most suitable for vote confirmation?

	Very suitable	Suitable	Neither	Not suitable	Absolute not suitable	Don't know
• SMS	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Elections web-page	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Different webpage	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Other _____	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

18. Does the information that safe communication canal in e-voting system is used would increase your trust in e-voting?

Yes, very much	Yes	Neither	No	Absolutely no	I do not have opinion
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

19. Does the information that vote is transferred using cryptographic method would increase your trust in e-voting system?

Yes, very much	Yes	Neither	No	Absolutely no	I do not have opinion
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

20. Would you agree to download free antivirus program to scan your computer before voting?

Yes, very much	Yes	Neither	No	Absolutely no	I do not have opinion
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

21. Does system's audit would help to increase trust in e-voting systems?

Yes, very much	Yes	Neither	No	Absolutely no	I do not have opinion
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

22. What help and assistance tools during e-voting would increase your trust in e-voting systems?

	Very important	Important	Neither	Not important	Absolute important	Don't know
• Demo version	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• On-line help	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Phone help	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• FAQ	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Other _____	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

23. Please evaluate does the system should have possibility to recalculate votes?

Yes, absolutely	Yes	Neither	No	Absolutely no	I do not have opinion
-----------------	-----	---------	----	---------------	-----------------------

Yes, absolutely	Yes	Neither	No	Absolutely no	I do not have opinion
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

24. Please evaluate how crucial is fact that votes can't be published before the end of elections?

Very important	Important	Neither	Not important	Not important at all	I do not have opinion
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

25. Please evaluate how is important in e-voting system to make competent representers of elections institutions eligible to participate in final vote calculation?

Very important	Important	Neither	Not important	Not important at all	I do not have opinion
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

2 PRIEDAS

Anketa (lietuviška versija)

Laba diena, gerbiamas (-oji) respondente. Aš, Vilniaus universiteto Kauno humanitarion fakulteto studentė atlieku tyrimą tema “PASITIKĖJIMO ELEMENTŲ ELEKTRONINIO BALSAVIMO SISTEMOMIS TYRIMAS”.

Mažėjantis rinkėjų aktyvumas skatina ieškoti būdų balsavimo procedūrai palengvinti. Elektroninės balsavimo sistemos yra vienas iš galimų sprendimų. Šis tyrimas skirtas suprasti faktorius, kurie lemia rinkėjų pasitikėjimą šiomis sistemomis. Po to sudaryti galimus scenarijus esamoms sistemoms patobulinti. Šio tyrimo metu surinkta informacija bus pateikta tik apibendrinta forma. Šioje anketoje Jūsų pateikti duomenys viešai nebus skelbiami. Maloniai prašome Jūsų atsakyti į pateiktus klausimus.

Dėkojame už Jūsų atsakymus.

1. Kokia Jūsų lytis?

- Moteris
- Vyras

2. Koks Jūsų amžius?

- Mažiau arba lygu 20
- 21-25
- 26-35
- 36-45
- 46-55
- 56-65
- Daugiau nei 65

3. Jūsų pastovi gyvenamoji vieta?

- Danija
- Vokietija
- Lietuva
- Lenkija
- Prancūzija
- Italija
- Kita _____

4. Koks Jūsų išsilavinimas?

- Vidurinė mokykla
- Aukštasis neuniversitetinis
- Aukštasis universitetinis
- Magistro laipsnis
- Kita_____

5. Koks Jūsų naudojimosi kompiuteriu lygis?

- Nesinaudoju kompiuteriu
- Vidutinis
- Patyręs vartotojas
- Ekspertas

6. Ar naudojate el. valdžios paslaugomis?

- Yes
- No

7. Jei atsakėte taip, kuriomis paslaugomis naudojate?

- Nesinaudoju
- Ieškoti informacijos
- Parsisiųsti formas ir medžiagas
- Mokėti mokesčius
- Užsisakyti pasą/ vairuotojo pažymėjimą
- Registruoti automobilį
- Mokėti sąskaitas
- Balsuoti
- Kita_____

8. Kuris balsavimo būdas Jums priimtinausias?

- Įprastas balsavimo apylinkėse (paper based)
- El. balsavimas
- Balsavimas paštu
- Kiti_____

9. Kokia Jūsų nuomonė, ar reikalinga įdiegti el. balsavimo sistema Jūsų šalyje?

- Taip
- Ne

10. Jei atsakėte taip, prašau pažymėti priežastis dėl ko manote ji reikalinga.

- Asmenys atsakingi už balsadėžes gali įtakoti rinkimų rezultatus

- Balsų skaičiavimo laikas per ilgas
- Valdžia gali paveikti rinkimų rezultatus manipuliudama jais
- Mažėjantis rinkimuose dalyvaujančių piliečių skaičius
- Piliečiai užsienį vangiai eina į rinkimus

11. Kas Jūsų nuomone turi kurti ir palaikyti el. balsavimo sistemą?

- Vietinė kompanija
- Valdžios institucija
- Užsienio kompanija

12. Kaip Jūs manote, ar pasitikėtumėte el. balsavimo sistemomis?

- Taip
- Ne

13. Prašome įvertinti rodiklių svarbą, lemiančių Jūsų pasitikėjimą el. balsavimo sistema.

	Labai svarbu	Svarbu	Nei svarbu, nei nesvarbu	Nesvarbu	Visiškai nesvarbu	Neturiu nuomonės
• Identifikacija	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Sistemos skaidrumas	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Pakartotinis balsavimas	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Rinkėjo konfidencialumas	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Visapusiška pagalba	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• El. bankininkystės panaudojimas el. balsavimo sistemoje	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Pasitikėjimas valdžios institucijomis ir rinkimais	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

14. Ar pasitikite Jūsų šalies valžia bei rinkimais?

		Nei				
		pasiti				
Taip, visiškai pasitikiu	Taip, pasitikiu	kiu, nei nepasitikiu	Nepasitikiu	Visiškai nepasitikiu		Neturiu nuomonės
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>		(6) <input type="checkbox"/>

15. Įvertinkite kaip rinkėjas iš pasitikėjimo sistema pozicijos šiuos rinkėjo autentifikacijos būdus:

				Nei		
				pasitikiu		
	Labai pasitikiu	Pasitikiu		, nei nepasitikiu	Visiškai nepasitikiu	Neturiu nuomonės
				nepasiti		
				kiu		
• Login ir slaptažodis	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Nutrinami kodai	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Skaitmeninis parašas	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Biometrinis identifikavimas	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• E-bankininkystės sistema	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Kita _____	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

16. Ar Jums kaip rinkėjui reikia patvirtinimo, jog Jūsų balsas buvo užregistruotas?

- Taip
- Ne

17. Jei atsakėte taip, prašome įvertinti įrankių tam atlikti tinkamumą:

				Nei		
				tinkam		
	Labai tinkamas	Tinkamas		as, nei as netinkamas	Netinkamas	Visiškai netinkamas
						Neturiu nuomonės

	Labai tinkamas	Tinkamas	Nei tinkamas, nei netinkamas	Netinkamas	Visiškai netinkamas	Neturiu nuomonės
• SMS	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Rinkimų puslapis	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Kitas nei rinkimų puslapis	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Kitas _____	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

18. Ar informavimas, kad el. balsavimo sistema naudoja saugų ryšio kanalą balso perdavimui padidintų Jūsų pasitikėjimą sistema?

Taip, labai	Ne	Nei taip, nei ne	Ne	Visiškai ne	Neturiu nuomonės
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

19. Ar informavimas, kad balsas užšifruotas perdavimo metu saugiu kriptografiniu metodu, padidintų pasitikėjimą el. balsavimo sistema?

Taip, labai	Taip	Nei taip, nei ne	Ne	Visiškai ne	Neturiu nuomonės
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

20. Ar sutiktumėte parsisiųsti nemokamą antivirusinę programą iš rinkimų puslapio ir perskanuoti Jūsų kompiuterį prieš balsuojant?

Taip, labai	Taip	Nei taip, nei ne	Ne	Visiškai ne	Neturiu nuomonės
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

21. Ar sistemos auditas padėtų padidinti pasitikėjimą el. balsavimo sistema?

Taip, labai	Taip	Nei taip, nei ne	Ne	Visiškai ne	Neturiu nuomonės
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

22. Kokie pagalbos įrankiai skirti vartotojo pagalbai padėtų pasitikėti el. balsavimo sistema?

	Labai svarbu	Svarbu	Nei svarbu, nei nesvarbu	Nesvarbu	Visiškai nesvarbu	Neturiu nuomonės
• Demo versija	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• On-line pagalba	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Telefono pagalba	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• DUK	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>
• Kita _____	(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

23. Ar sistemoje turi būti realizuotas balsų perskaičiavimas?

Taip, labai	Taip	Nei taip, nei ne	Ne	Visiškai ne	Neturiu nuomonės
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

24. Kaip svarbu, kad rinkimų balsai nebūtų paviešinti prieš rinkimų pabaigą?

Labai svarbu	Svarbu	Nei taip, nei ne	Nesvarbu	Visiškai nesvarbu	Neturiu nuomonės
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

25. Kaip svarbu, kad kompetetingi rinkimų komisijos atsovai galėtų dalyvauti balsų skaičiavime:

Labai svarbu	Svarbu	Nei taip, nei ne	Nesvarbu	Visiškai nesvarbu	Neturiu nuomonės
(5) <input type="checkbox"/>	(4) <input type="checkbox"/>	(3) <input type="checkbox"/>	(2) <input type="checkbox"/>	(1) <input type="checkbox"/>	(6) <input type="checkbox"/>

3 PRIEDAS

PASITIKĖJIMO ELEMENTŲ EL. BALSAVIMO SISTEMOSE TYRIMAS

Ginta Šolytė

*Vilniaus Universitetas Kauno Humanitarinis fakultetas, Muitinės g. 8, LT-44280, Kaunas, Lietuva,
asolyte@yahoo.com*

Santrauka. Straipsnis apžvelgia atliktą tyrimą, kurio metu buvo siekiama nustatyti pasitikėjimo elementus el. balsavimo sistemose ir pasiūlyti jų diegimo galimybes. Visų pirma buvo išnagrinėti el. valdžios pasitikėjimą tiriantys modeliai. Po to buvo išskirti pasitikėjimą el. balsavimo sistemomis kuriantys veiksniai. Sukurtas el. balsavimo sistemos modelis, skirtas sustiprinti vartotojo pasitikėjimą. Atliktas eksperimentinis tyrimas - el. balsavimo sistemų vartotojų apklausa, siekiant įvertinti veiksnius, turinčius teigiamą įtaką vartotojų pasitikėjimui.

Raktažodžiai: el. valdžia, el. balsavimas, pasitikėjimas, rinkėjas.

Ivadas

Viešojo administravimo srityje poreikis adaptuoti valdžios veiklas siekiant atsakyti į vyraujančias tendencijas yra jaučiamas daugelyje šalių. Vienas iš sudėtingiausių el. valdžios projektų - el. balsavimas. Balsavimas yra vienas iš svarbiausių procesų mūsų demokratinėje visuomenėje, teikiantis tiesioginį demokratijos kanalą piliečiams taip pat sutvirtinantis rinkėjų pasitikėjimą valdžios institucija. El. balsavimas tai paprastai nestebimas, nepriklausantis nuo vietos rinkimų kanalas leidžiantis rinkėjams balsuoti iš jų elektroninių įrengimų. El. balsavimo šalininkai argumentuoja, kad el. balsavimas leistų pasiekti teigiamus efektus: padidintų neturinčių palankių sąlygų balsuoti bendruomenių dalyvavimą rinkimuose; sumažintų rinkėjų apatiškumą; suteiktų didesnę patogumą rinkėjui, balsavimo laiko ir vietos atžvilgiu; tai būtų galimybė žmonėms su negalia patogiau balsuoti, sutaupytų pinigų ir pasiektų didesnę tikslumą [4].

El. balsavimo bandymai yra įvykdyti JAV, Didžiojoje Britanijoje, Šveicarijoje, Ispanijoje, Prancūzijoje, Nyderlanduose. Vienas iš pirmųjų stambių el. balsavimo eksperimentų buvo atliktas JAV - (SERVE), tačiau dėl rimtų saugumo spragų sistemos buvo atsisakyta. Šveicarijoje elektroninio balsavimo eksperimentai buvo įvykdyti trijuose kantonuose 2003 m., taip pat penki bandomieji balsavimai įvykdyti 2004 ir 2005 m. nacionaliniuose referendumuose. Estijoje balsavimas internetu buvo panaudotas 2005 m. savivaldos ir 2007 m. parlamento rinkimuose. Lietuvoje 2006 m. Seimas patvirtino balsavimo internetu rinkimuose ir referendumuose koncepciją, o 2007 m. Vyriausybė patvirtino balsavimo internetu diegimo programą ir pavedė ją koordinuoti Informacinės visuomenės plėtros komitetui.

Sėkmingas el. valdžios projektų diegimas ir valdymas priklauso nuo sėkmingo svarbiausių elementų – žmonių, technologijos, organizacijos ir finansinių resursų, teisinių bei politinių sąlygų suderinimo. Svarbu pažymėti, kad el. valdžios projektai privalo būti orientuoti į valdžios institucijos darbuotoją bei galutinį vartotoją - pilietį. Vienas iš svarbiausių faktorių lemiančių el. valdžios pasisekimą yra piliečių noras priimti šias sistemas ir dalyvauti procese [9]. Atlikti tyrimai rodo, kad svarbiausias veiksnys, lemiantis vartotojų norą priimti el. valdžios paslaugas yra pasitikėjimas jomis, tačiau pasitikėjimo koncepcija yra labai sudėtinga ir reikalauja išsamaus tyrimo.

Atlikto darbo mokslinė problema - kokie veiksniai kuria pasitikėjimą el. balsavimo sistemomis? Straipsnio tikslas - aprašyti atliktą tyrimą, tiriantį pasitikėjimą kuriančius elementus elektroninėse balsavimo sistemose. Pirmiausia, apžvelgiami pasitikėjimą el. valdžios paslaugose tiriantys modeliai, po to pateikiamas apibendrintas el. balsavimo sistemų modelis su pasitikėjimą kuriančiais veiksniais, paskutinioji dalis aprašo eksperimentinį tyrimą, tiriantį modelio veiksmumą bei pateikiamos išvados apie gautus rezultatus.

Pasitikėjimo samprata el. valdžios modeliuose

Pasitikėjimą sudėtinga išmatuoti tiesiogiai; paskutiniu metu jis išsivystė iš statistinės į dinaminę koncepciją su skirtingomis charakteristikomis bei vystymosi etapais [9]. Siekiant sukurti pasitikėjimą el. balsavimu, reikalinga suprasti faktorius, kurie įtakoja piliečio pasitikėjimo formavimosi procesus.

Apžvelgus pasitikėjimą el. valdžia tiriančių autorių darbus, pasitikėjimą kuriančius faktorius galima suskirstyti į dvi grupes: prieš sąveiką su sistema ir sąveikos metu. Pasitikėjimo el. valdžia modelis susideda iš stebinčio vartotojo (piliečio), pasitikėjimą teikiančio objekto (el. valdžios sistemos) ir aplinkos (technologijų ir trečiosios šalies). Lentelėje 1 pateikiami sugrupuoti požymiai pagal požymių tipus.

Lentelė 1. Pasitikėjimo el. valdžia faktoriai

Veikimo laikas	Požymių tipas	Požymiai
Prieš sąveiką	Individualaus piliečio elgesio požymiai	Subjektyvios normos, individuali demografija, polinkis į el. valdžią, pažinimo procesas, bendros intencijos pasitikėjimui ir el. paslaugų naudojimas; kitų asmenų nuomonė, patirtis, susipažinimas su sistema, individuali kultūra bei tradicijos [3,9,11].
	Instituciniai požymiai	Organizacijos reputacija, akreditacija, bendrai suvokiamas organizacijos patikimumas, autentifikavimas, vartotojų bendruomenės, įstatyminiai reikalavimai, autoritetas ir kompetencija [3,6,9].
	Technologiniai Požymiai	Perdavimo kokybė, sąsajos dizainas ir sudėtis, saugumas, abipusiškumas, skaitmeninis sertifikatas, viešojo rakto infrastruktūra, autentiškumas, vientisumas, struktūriniai garantai, neanuliuotumas, kompetencija ir nuspėjamumas, privatumas, tranzakcijos nuoseklumas, prieinamumas ir konfidencialumas [3,6,8,9].
Sąveikos metu	Paslaugos požymiai	Ilgaamžiškumas, patikimumas, pritaikomumas individualiam vartotojui, prieinamumas ir kokybė: informacija, vartotojo sąsajos draugiškumas ir estetika [3,9,10].
	Tranzakcijos išpildymo požymiai	Skaidrumas, aptarnavimas po tranzakcijos įvykdymo, tikslumas ir kokybė [3,9].
	Informacijos savybės	Tikslumas, išbaigtumas, nešališkumas, patikimumas, aplinka, naudingumas ir kokybė [3,6,9].

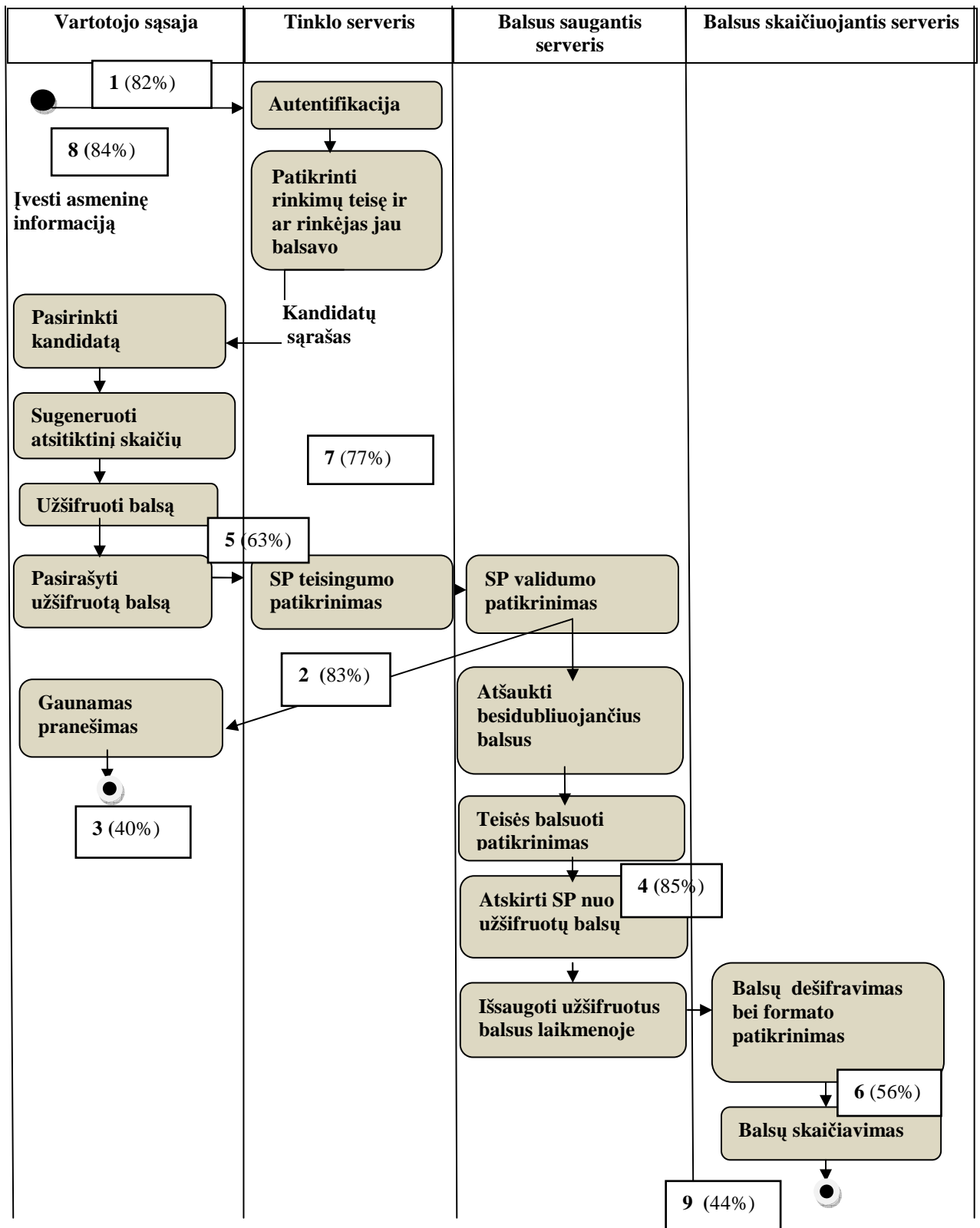
Warkentin (2002) teigia, jog vartotojas rinkdamasis naudotis sistema ar ne suvokia riziką ir įvertina potencialią naudą. Pasitikėjimas yra sukurtas per pasikartojančius procesus ir paremtas institucija, jis pastoviai auga per asmens suinteresuotumą. Svarbu sertifikavimas apie patikimumą ir numatytas asmens elgesys, išpareigojimai, kurie garantuoja sąveikos rezultatus. Turi būti vykdoma kontrolė, kaip informacija bus valdoma [11]. Riedl (2004) teigia, kad duomenų perdavimas bei privatumo užtikrinimas veikia kaip pagrindinis veiksnys. Pasitikėjimas valdžios institucijomis tiesiogiai veikia pasitikėjimą, nuostatas ir reputaciją el. valdžios atžvilgiu [7]. Evans ir Yen (2005) labiausiai akcentuoja: neautorizuoto priėjimo riziką, viešojo rakto infrastruktūrą ir metodus autentifikacijai, sunkumus komunikuojant su el. valdžia [2]. Carter (2005) teigia, kad naudojimosi paprastumas, suderinamumas ir patikimumas yra svarbiausia kuriant pasitikėjimą [1]. Parent (2005) įvardina, kad pasitikėjimą valdžia didina - padidėjęs veiksmingumas, skaidrumas ir sąveika [8]. Teo (2008) pažymi, kad sistemos patikimumas, kompetencija ir saugumas, tikslumas bei pateikimas laiku yra svarbiausi veiksniai [10].

3 Pasitikėjimą el. balsavimu kuriantis modelis

Šiame skyrelyje apžvelgiamas pasiūlytas modelis, kurio esminis skirtumas nuo esamų modelių yra pasitikėjimo elementų identifikavimas ir įjungimas į el. balsavimo scenarijaus etapus. Modelis sukurtas remiantis nagrinėtomis Estijos bei Šveicarijos el. balsavimo sistemomis bei pritaikant nagrinėtoje literatūroje apibendrintą el. balsavimo sistemos pasitikėjimo modelį. Ši sistema susideda iš vartotojo sąsajos, tinklo serverio bei serverių, kurie saugo, apdoroja bei skaičiuoja balsus. El. balsavimo sistemoje vykstančius procesus galima suskirstyti į šešis pagrindinius etapus: registraciją, autentifikaciją, balsavimą ir balsų saugojimą, balsų tvarkymą, balsų skaičiavimą bei auditą [5]. Modelio struktūra pateikta Pav.1

Pasitikėjimą kuriantys elementai: (1) **Sistemos tikslumas** – išreikštas per patikimą **autentifikaciją**, kuomet asmuo, dalyvaujantis rinkimuose identifikuojamas kaip asmuo, kuris jis skelbiasi esąs. Tik asmenys, turintys teisę balsuoti gali dalyvauti rinkimuose ir asmenys neturintys teisės balsuoti negali dalyvauti rinkimuose. Nagrinėtose sistemose vykdomas skirtingai, tačiau saugiausias iš jų ID kortelės su skaitmeniniu parašu panaudojimas. (2) **Sistemos skaidrumas** - rinkėjai privalo žinoti, jog jų balsai bus įskaičiuoti į galutinį rezultatą. Sistemoje realizuojamas atsiunčiant bei sukuriant informatyvią pakartotinio prisijungimo posistemę. (3) **Pakartotinis balsavimas** – realizuotas pakartotinis balsavimas rinkėjui pakeitus pasirinkimą, tačiau užtikrinamas prieš tai buvusio balso išėmimas iš sistemos ir rinkėjo balsas gali būti įskaičiuotas į galutinį balsų skaičiavimą tik vieną kartą. Prieš balsuojant rinkėjas balsavimo puslapyje aiškiai informuojamas, kad balsuoti galima daugiau nei vieną kartą, pakeitus apsisprendimą. (4) **Rinkėjų konfidencialumas** – balsus skaičiuojančiame serveryje atskirai saugoma rinkėjo asmeninė informacija bei jo balsas. Be to atskirtų balsų bei rinkėjų ID sąrašai nuolatos maišomi siekiant atsitiktinio generavimo bei siekiant nutraukti bet

kokius mėginimas susieti šiuos du sąrašus. 5) **Sistemos saugumas** - perdavimo kanalas tarp rinkėjo ir serverio turi būti saugus, rinkėjai turi būti tikri, kad jų balsai nusiųsti į oficialų serverį ir, kad balsai apsaugoti nuo trečiosios šalies priėjimo. Šifravimui naudojami kriptografiniai metodai bei saugaus ryšio kanalo panaudojimas balso perdavimui. Reikalingi dėl to, kad rinkėjai jaustųsi saugūs pateikdami savo pasirinkimą. (6) **Sistemos slaptumas** - rinkėjų pasirinkimas nebus atskleistas jokiais aplinkybėmis. Realizuotas panaudojant jau minėtas saugumo priemones bei dešifravimui reikalingą privatų raktą padalinus tarp įgaliotų rinkimų komisijos atstovų. Apie šią el. balsavimo sistemos veikimo dalį, rinkėjai turi būti informuojami prieš balsavimo procesą. (7) **Pakankamos pagalbos** rinkėjams užtikrinimas: pagalba išdėstyta patogiai lange, į ją kreipiamasi bet kuriuo metu, be to, rinkėjas gali grįžti atgal visame balsavimo procese. Reikalinga dėl sistemos suprantamumo ir adaptavimo rinkėjui. (8) **Pasitikėjimas valdžia** - išsami informacija apie sistemos kūrėją, atvaizduojama vartotojo sąsajoje prieš autentifikaciją. Jis yra svarbus kaip institucinis požymis, veikiantis piliečio elgesį bei apsiprendimą. (9) **Auditas** - informacija, kad sistema audituojama viso proceso metu. Reikalinga dėl sistemos patikimumo. Informavimas apie balsų perskaičiavimo galimybę. Balsai saugomi ir pririnkus perskaičiuojami, užtikrinamas papildomas sistemos auditas.



Pav.1 Pasitikėjimą didinantis el. balsavimo sistemos modelis

4 Eksperimentinis tyrimas

Atliktas eksperimentinis tyrimas vyko Aalborg mieste, Danijoje. Buvo apklausti 110 nuo 18 iki 35 m. universiteto studentų, skirtingų lyčių, išsilavinimo, gyvenamosios vietos, naudojamasi kompiuteriu lygio. Anketos klausimai buvo sudaryti, siekiant patikrinti pasitikėjimą el. balsavimo sistemomis kuriantį modelį ir siekiant išsiaiškinti,

kurie pasiūlyti elementai yra svarbiausi, o kurie vartotojui įtakos nedaro. Nagrinėtose sistemose apžvelgti elementai naudojami skirtingai, buvo iširta, kurie elementai būtini vartotojo atžvilgiu, sekančiai vaizduojami pagal gauto tyrimo rezultatus sureitinguoti pasitikėjimo elementai, mažėjimo tvarka:

- 1) **(4) Rinkėjo konfidencialumas** svarbus (85%) apklaustųjų.
- 2) **(8) Pasitikėjimas valdžia** - 84% apklaustųjų įvardijo, kaip svarbų faktorių. 51% apklaustųjų naudojami el. valdžios paslaugomis, net 53% apklaustųjų mano, kad el. balsavimas reikalingas įdiegti jų šalyse. Be to, tinkamiausiu el. balsavimo sistemos kūrėju bei palaikytoju, respondentai laiko valdžios instituciją 61%.
- 3) **(2) Sistemos skaidrumas** išreikštas per patvirtinimą apie balso užregistravimą (83%). Be to priimtinausias būdas patvirtinti, kad balsas buvo užregistruotas yra rinkimų puslapis (66%).
- 4) **(1) Rinkimų tikslumas** – rinkėjo autentifikacija (82%). Autentifikacijai labiausiai tinkama ID kortelė su skaitmeniniu parašu (71%) bei prisijungimo vardas su slaptažodžiu (63%). Apklaustieji įvardijo, kad nutrinamų kodų kortelė bei e-bankininkystės sistema autentifikacijai netinkama.
- 5) **(7) Pagalba**, tinkamiausia pagalba - online pagalba (77%), pagalba telefonu (65%) bei DUK (59%).
- 6) **(5) Sistemos saugumas** - informavimas, jog balsas užšifruotas kriptografiniu metodu (62%) ir sistema naudoja saugų ryšio kanalą perdavimui (63%).
- 7) **(6) Sistemos slaptumas** - kompetingų rinkimų komisijos atstovų dalyvavimas balsų skaičiavime (56%).
- 8) **(9) Auditas** - sistemos auditas, svarbus elementas tik 44% apklaustųjų, - informavimas apie balsų perskaičiavimo galimybę 66% apklaustųjų.
- 9) **(3) Pakartotinis balsavimas** svarbus elementas 40% apklaustųjų.

Išvados

Straipsnyje apibendrinti el. valdžios paslaugose pasitikėjimą kuriantys elementai. Iširtos el. balsavimo sistemų savybės ir išskirti vartotojo pasitikėjimą įtakojantys elementai. Sudarytas pasitikėjimo užtikrinimo el. balsavimo sistemose modelis, atliktas eksperimentinis tyrimas, kuris leido įvertinti šių elementų svarbą, išsiaiškinti vartotojų prioritetams bei nuostatas apie pasitikėjimo stiprinimą visuose el. balsavimo scenarijaus etapuose. Svarbiausias veiksnys apklaustiems yra rinkėjo konfidencialumas, po to pasitikėjimas valdžia, trečiasis faktorius - patvirtinimas apie balso užregistravimą. Ketvirtas elementas - rinkėjo autentifikacija, penktas – pagalba, šeštasis – sistemos saugumas. Buvo nustatyta, kad rinkėjams nėra svarbu sistemos auditavimas, kompetingų rinkimų komisijos atstovų dalyvavimas balsų skaičiavime bei pakartotinio balsavimo galimybė.

Literatūros sąrašas

- [1] **Carter L., Belanger F.** The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information Systems Journal*. 2005, volume 15, pp. 5-25.
- [2] **Evans D., Yen D. C.** E-government: An analysis for implementation: Framework for understanding cultural and social impact. *Government Information Quarterly*. 2005, volume 22, pp. 354–373.
- [3] **Kim D. J., Song Y. I., Braynov S.B., Rao H.R.** A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/practitioner perspectives. *Decision Support Systems*. 2005, volume 40, pp. 143-165.
- [4] **Lauer T. W.** The Risk of e-Voting. *Electronic Journal of e-Government*. 2004, volume 2, no. 3, pp. 177-186.
- [5] **Mägi T.** Practical Security Analysis of E-voting Systems. *Talinas: University of Technology*, 2007, [interaktyvus], [žiūrėta 2009 m. vasario 27 d.]. Prieiga per internetą: <http://triinu.net/e-voting/master%20thesis%20e-voting%20security.pdf>.
- [6] **McKnight D.H., Choudhury V., Kacmar C.** The Impact of Initial Consumer Trust on Intentions to Transact with Web Sites: A Trust Building Mode. *Journal of Strategic Information Systems*. 2002, volume 11, pp. 297–323.
- [7] **Riedl R.** Rethinking trust and confidence in European e-government. *IEEE Proceedings*. 2004, [interaktyvus], [žiūrėta 2009 m. vasario 27 d.]. Prieiga per internetą: http://www.ifi.unizh.ch/egov/Trust_v1.0.pdf.
- [8] **Parent M., Vandebek C.A., Gemino A.C.** Building citizen trust through e-government. *Government Information Quarterly*. 2005, volume 22, pp. 720-736.
- [9] **Tassabehji R., Elliman T.** Generating citizen trust in e-Government using a trust verification agent: a research note. *European and Mediterranean Conference on Information Systems (EMCIS)*, 2006.
- [10] **Teo.T.S.H., Srivastava S.C., Jiang L.** Trust and Electronic Government Success: An Empirical Study. *Journal of Management Information Systems*. 2008, volume 25, no. 3, pp. 99-131.
- [11] **Warkentin M., Gefen D., Pavlou P. A., Rose G. M.** Encouraging Citizen Adoption of e-Government by Building Trust. *Electronic Markets*. 2002, volume 12, no. 3, pp. 157-162.

VILNIAUS UNIVERSITETAS
KAUNO HUMANITARINIS FAKULTETAS
INFORMATIKOS KATEDRA

VERSLO INFORMACINIŲ SISTEMŲ MAGISTRANTŪROS PROGRAMOS
MOKSLO TIRIAMOJO DARBO PLANAS

Magistrantė: Ginta Šolytė Tel. +370 (648) 314 18

(vardas, pavardė)

Magistrantūros studijų trukmė: 2007 m. - 2009 m.

TEMA: PASITIKĖJIMO ELEMENTŲ ELEKTRONINIO BALSAVIMO SISTEMOMIS
TYRIMAS.

Vadovė: Dalia Krikščiūnienė, Doc. Dr. VU KHF Informatikos katedra

Darbo anotacija:

Tikslas: ištirti elektroninio balsavimo sistemų pasitikėjimo veiksnius ir jų įdiegimo IS prielaidas.

Uždaviniai:

- 1) Išanalizuoti kriterijus, kuriais remiantis nustatomas pasitikėjimas elektroninio balsavimo sistemomis.
- 2) Išnagrinėti esamose elektroninio balsavimo sistemose Estijoje bei Šveicarijoje ir Lietuvos teoriniame modelyje, egzistuojančius pasitikėjimą kuriančius veiksnius.
- 3) Pasiūlyti specializuotą apimantį tiek technologinius, tiek socialinius aspektus pasitikėjimą elektroninėmis balsavimo sistemomis nustatantį metodą, įdiegiamą IS.
- 4) Atlikti ekperimentinį tyrimą ir įvertinti pasiūlyto metodo taikymo galimybes. Eksperimentas susidarys iš EBS su pasitikėjimą didinančiomis priemonėmis analizės. Bus vertinama ar tokia sistema vartotojai pasitiki labiau.

Metodai, kuriuos ketinama ištirti ir panaudoti darbe: nagrinėjama mokslinė literatūra ir atliekama jos analizė bei apibendrinimas. Kuriamas ekperimentinis modelis patikrinti ar nustatyti veiksniai įtakoja pasitikėjimą sistemomis. Jis susidarys iš EBS pasitikėjimą veikiančių veiksnių analizės. Bus atliekamas kokybinis tyrimas, kuris sieks patikrinti ar siūlomi veiksniai veikia vartotojus, atskleisti kokie dar neįtraukti į sąrašą veiksniai įtakoja rinkėjų pasirinkimą. Tyrimo metodai: pokalbis ar interviu su keletu ekspertų. Apibendrinus rezultatus ir sudarius tikslesnį veiksnių sąrašą, anketiniu

būdu bus tiriami rinkėjai. Bus siekiama anketos metodu nustatyti ar siūlomos pasitikėjimą didinančios priemonės įtakoja rinkėjų pasirinkimą.

Laukiami rezultatai: Ištirti pasitikėjimą elektroninio balsavimo sistemomis įtakojančius veiksniai, IS įdiegimas.

Mokslo - tiriamojo darbo planas

Semestras	(data)	Užduotys
S1	2007.09.20	Preliminarios magistrinio darbo temos formulavimas.
	2007.10.25	Literatūros šaltinių parinkimas.
	2007.11.30	Literatūros šaltinių analizė, grupavimas, pagrindinių idėjų apžvalga.
	2007.12.01	Eksperimentinių duomenų paieška.
	2007.12.30	Magistrinio darbo įvado rašymas.
	2008.01.22	Ataskaitos pristatymas ir gynimas.
S2	2008.02.28	Teorinės dalies rašymas.
	2008.03.25	Pasitikėjimą sistemomis parodančių kriterijų paieška ir susisteminimas.
	2008.04.10	Elektroninių balsavimo sistemų lyginamoji analizė: privalumai bei trūkumai.
	2008.06.10	Siūlomas specializuotas sistemos pasitikėjimą nustatantis metodas.
	2008.06.20	Ataskaitos pristatymas ir gynimas.
S3	2008.09.20	Tyrimo metodikos ruošimas eksperimentinei daliai.
	2008.10.25	Straipsnio konferencijai rašymas.
	2008.11.30	Duomenų ir kitos eksperimentiniam tyrimui reikalingos medžiagos rinkimas, apdorojimas ir įvertinimas.
	2008.12.01	Eksperimentinio tyrimo atlikimas.
	2009.01.20	Eksperimentinio tyrimo rezultatų įvertinimas.
	2009.01.30	Išvados.
	2009.02.03	Ataskaitos pristatymas ir gynimas.
S4	2009.04.01	Darbo taisymas, tobulinimas
	2009.05.01	Išvadų rašymas.
	2009.05.08	Straipsnio pristatymas
	2009.05.10	Prezentacijos ruošimas.
	2009.05.18	Galutinės ataskaitos pristatymas ir gynimas.

Magistrantas Vadovas:.....

(parašas)

(parašas)