ISSN 2029-7564 (online)
SOCIALINĖS TECHNOLOGIJOS
SOCIAL TECHNOLOGIES
2012, 2(2), p. 376–389

ELEKTRONINIŲ RINKIMŲ SISTEMŲ KONSTRAVIMO PRINCIPAI, MODELIAI IR JŲ APSAUGOS UŽTIKRINIMAS

Tadas Limba

Mykolo Romerio universitetas, Lietuva, limba@mruni.eu

Konstantin Agafonov

Mykolo Romerio universitetas, Lietuva, ka1979@gmail.com

Abstraktas

Tikslas – *išanalizuoti elektroninių rinkimų sistemų konstravimo principus, elektroninių rinkimų sistemų modelių kūrimo ir diegimo ypatumus, atskleisti elektroninių rinkimų pažeidimo metodus bei jų apsaugos užtikrinimo galimybes.*

Metodologija – *nagrinėjant anksčiau nurodytus elektroninių rinkimų sistemų konstravimo principus ir elektroninių rinkimų sistemų modelius, taikyti sisteminės analizės bei koncepcinės lyginamosios analizės metodai leidžia geriau atskleisti elektroninių rinkimų pažeidimų metodus bei nustatyti jų technologinės apsaugos užtikrinimo priemones.*

Rezultatai – *atskleisti elektroninių rinkimų sistemų pagrindiniai kūrimo, konstravimo principai, atlikta elektroninių rinkimų sistemų modelių lyginamoji analizė, sudaranti prielaidas kurti, plėtoti naujus modelius šioje srityje bei taikyti naujas ir efektyvias elektroninių rinkimų sistemų apsaugos nuo galimų pažeidimų priemones, laiku sukurti apsaugos nuo šių pažeidimų tarptautinius ir nacionalinius standartus.*

Praktinė reikšmė – *atlikus elektroninių rinkimų sistemų kontstravimo principų sisteminę analizę bei lyginamuoju aspektu išanalizavus elektroninių rinkimų sistemų modelius*

ISSN 2029-7564 (online)
https://www.mruni.eu/lt/mokslo_darbai/st/apie_leidini/
https://www.mruni.eu/en/mokslo_darbai/st/apie_leidini/index.php

išryškėję tam tikri privalumai ir trūkumai leistų efektyviau į įvairių šalių valstybės valdymo sistemas integruoti naujai kuriamus elektroninių rinkimų modelius, apibrėžiant šių modelių taikymo ypatumus svarbiausiuose strateginuose dokumentuose ir kituose nacionaliniuose teisės aktuose.

Originalumas – *darbo originalumą straipsnyje atspindi elektroninių rinkimų sistemų konstravimo ypatumų sisteminė analizė, išskiriant šešis pagrindinius bendruosius ir svarbiausius šių sistemų konstravimo principus, įvairių pasaulio mokslininkų sukurtų ir siūlomų elektroninių balsavimo (rinkimų) sistemų modelių koncepcinė analizė, šių modelių bendrųjų privalumų ir trūkumų išskyrimas lyginamuoju aspektu. Mokslinio straipsnio originalumas taip pat atsispindi elektroninių rinkimų modelių įgyvendinimo kontekste analizuojant aktualius klausimus, susijusius su grėsmėmis, kylančiomis elektroninių rinkimų sistemoms ir galimiems šių sistemų kompromitavimo metodams.*

Raktažodžiai – *internetas, informacinės technologijos, informacinės sistemos, elektroniniai rinkimai, elektroninis balsavimas, elektroninių rinkimų sistemos, elektroninių rinkimų modeliai, elektroninių rinkimų konstravimo principai, visuomenė.*

Tyrimo tipas – *e. rinkimų sistemų konstravimo principų, modelių ir šių sistemų pažeidimų bei apsaugos problematikos pristatymas.*

1. Įvadas

Elektroninis balsavimas dažniausiai interpretuojamas kaip galimybė gyventojams pateikti nuomonę įvairiais klausimais skirtingose visuomeninio gyvenimo srityse šiuo tikslu panaudojant ir pritaikant naujausias informacines komunikacines technologijas. Tokios balsavimo sistemos yra gana naujos, nors pačių automatizuotų balsavimo sistemų atsiradimo idėjos buvo pristatytos gana seniai. 1955 metais Erichas Fromas charakterizavo situaciją, kurioje asmenys, dalyvaujantys susitikimuose pasinaudoję techniniais įrenginiais, galėjo pareikšti savo nuomonę apie tam tikrus visuomenės susitikimuose svarstytus klausimus, o pirmoji sistema, kuri buvo panaši į kompiuterinę elektroninio balsavimo sistemą, buvo Murray Turoff 1970 metais sukurta EMISARI (angl. *Emergency Management Information System and Reference Index*) sistema, kuri buvo skirta kompiuterinėms konferencijoms. Ši sistema leido vartotojams svarstyti jiems aktualius klausimus ir pareikšti savo nuomonę. Galima teigti, kad EMISARI sistema tapo ateities elektroninių informacijos apsikeitimo sistemų prototipu ir sudarė palankias sąlygas ateityje svarstyti elektroninių rinkimų įgyvendinimo galimybes (Krimmer et al., 2007).

Naujojo tūkstantmečio pradžia iš esmės susijusi ir su naująja elektroninio balsavimo (rinkimų) epocha. Laikotarpis nuo 2000 metų ir iki šių dienų iš esmės yra elektroninių balsavimų vystymo ir nesėkmių laikotarpis. Vienos šalys, pvz., Estija, yra sukūrusios ir naudoja savo rinkimų sistemą ir nesiruošia jos atsisakyti, o kitose šalyse, pvz., Nyderlanduose, atsisakoma tam tikrų elektroninių rinkimų technologijų. Šis laikotarpis elektroninių rinkimų raidoje yra įdomus tuo, kad ateityje galima sulaukti tam tikrų neti-

kėtų sprendimų: interneto technologijomis grįstos balsavimų sistemos gali tapti vienintelėmis rinkimams naudojamomis sistemomis, jos gali būti transformuojamos į mobilių technologijų balsavimo sistemas ir pan.

Tyrimo problema. Visame pasaulyje yra pastebimas rinkėjų aktyvumo sumažėjimas. Ypač sudėtinga darosi tradicines rinkimų technologijas naudoti gyventojams, trumpalaikiai reziduojantiems užsienio šalyse. Tokie šalių gyventojai faktiškai yra eliminuojami iš tradicinių rinkimų. Tradiciniai rinkimai vykdomi įprastiniu būdu nepritraukia visų rinkėjų, kadangi piliečiams, turintiems teisę dalyvauti rinkimuose, ne visuomet yra patogu apsilankyti rinkimų apylinkėse dėl laiko stokos ar dėl didelio atstumo iki jų. Būtent dėl šių priežasčių elektroniniai rinkimai, dar dažnai vadinami elektroniniais balsavimais (e. balsavimais), tampa patrauklesni tam tikrai rinkėjų auditorijai. Iš esmės terminas e. balsavimas yra globalus terminas, apimantis bet kokias rinkimų technologijas, grindžiamas elektroninių priemonių taikymu: balsavimas panaudojant elektronines balsų skaičiavimo mašinas arba rinkimai, organizuojami per elektroninius terminalus rinkimų apylinkėse, arba internetu vartotojams naudojantis kompiuteriais vykdomi rinkimai.

Tyrimo objektas – elektroninių balsavimo sistemų konstravimo principų ir šių sistemų modelių diegimas.

Tyrimo tikslas – išanalizuoti elektroninių rinkimų konstravimo principus, elektroninių rinkimų sistemų modelių kūrimo ir diegimo ypatumus, atskleisti elektroninių rinkimų pažeidimo metodus bei jų apsaugos užtikrinimo galimybes.

Uždaviniai:

1. išanalizuoti elektroninio rinkimų (balsavimo) sistemų konstravimo principus;
2. atlikti elektroninių rinkimų sistemų modelių lyginamąją analizę;
3. išnagrinėti elektroninių rinkimų saugumo problematiką;
4. atskleisti ir išanalizuoti elektroninių rinkimų sistemų pažeidimų metodus.

Darbo naujumą straipsnyje atspindi elektroninių rinkimų sistemų konstravimo principų sisteminė analizė, įvairių pasaulio mokslininkų sukurtų ir siūlomų elektroninių balsavimo (rinkimų) sistemų modelių koncepcinė analizė, šių modelių bendrųjų privalumų ir trūkumų išskyrimas lyginamuoju aspektu. Mokslinio straipsnio naujumas taip pat atsispindi analizuojant aktualius klausimus, susijusius su grėsmėmis, kylančiomis elektroninių rinkimų sistemoms ir galimiems šių sistemų kompromitavimo metodams.

2. Elektroninių rinkimų sistemų konstravimo principai

Politinių partijų ir įvairių valstybių vyriausybių atstovai įžvelgė, kad pasaulyje atsiradęs visuotinis interneto tinklas yra labai reikšmingas šiuolaikinei visuomenei ir šalyse vykstantiems politiniams procesams. Vienas garsiausių elektroninių rinkimų projektų įgyvendintas 1996 metais Brazilijoje vykusiuose parlamentiniuose rinkimuose (Krimmer et al., 2007). Nors tai ir buvo e. rinkimų sistema, kurios veikimui nebuvo naudotos interneto technologijos, ji tapo vėliau sukurtos internetinės balsavimo sistemos prototipu. 1998 metų Brazilijos rinkimuose dalyvavo apie 60 milijonų rinkėjų, o 57 procentai

jų balsavo elektroniniu būdu. Tais pačiais metais internetiniu balsavimu pasinaudojo JAV Reformatų partija, o internetu balsavo apie 2000 rinkėjų. Tai laikotarpis, kurio metu pasaulyje buvo inicijuota daugybė projektų ir atlikta daugybė mokslinių tyrimų, susijusių su elektroniniais rinkimais. Savo populiarumo viršūnę internetinės elektroninės balsavimo sistemos pasiekė 2001 metais (Volkamer and Hutter, 2004).

Galima teigti, kad balsavimai rinkimų metu ir įvairūs referendumai yra pagrindinis demokratinės visuomenės įrankis, kuris leidžia rinkėjams pakankamai aktyviai dalyvauti valstybių politiniuose procesuose. Didėjant visuotinės kompiuterizacijos ir informacinių bei telekomunikacinių technologijų naudojimo mastui, visuomenė pradeda domėtis ir šių technologijų panaudojimu šalies politiniame gyvenime. Internetiniai balsavimai yra vienas iš būdų mažiausiomis pastangomis „priversti“ didesnę visuomenės dalį aktyviai dalyvauti šalies politiniuose procesuose. Be abejonės, kad toks procesas būtų sklandus ir kuo didesnė visuomenės dalis dalyvautų naudojant naujas sistemas, visuomenei turi būti išaiškinti elektroninės rinkimų sistemos veikimo mechanizmai bei jos naudojimo principai.

Europos Tarybos Ministrų Komitetas 2004 m. rugsėjo 30 d. per 898-ąjį deleguotųjų ministrų susitikimą patvirtino Valstybių narių Ministrų Komiteto „Rekomendaciją (2004)11 dėl teisinių, organizacinių ir techninių normų, taikomų balsavimui rinkimuose elektroniniu būdu“ (Valstybės žinios, teisės akto Nr. X-912).

Pabrėžiant, kad balsavimo teisė yra vienas pagrindinių demokratijos principų, visi kiti demokratinių rinkimų ir referendumų principai turi būti išlaikomi ir įdiegus elektroninių rinkimų sistemas. Elektroniniai rinkimai turi būti tokie pat saugūs ir patikimi kaip ir įprastiniai, kuriuose nėra naudojamos šiuolaikinės elektroninės priemonės (Remmert, 2004). Kad elektroninės balsavimo sistemos taptų patrauklios visuomenei ir ateityje papildytų ar pakeistų įprastines (popierines) balsavimo sistemas, jose turi būti įgyvendinti šie esminiai ir neabejotinai svarbūs principai:

Visuomeniškumas ir visuotinis pripažinimas. Galimybė užtikrinti, kad visi balsavimo teisę turintys rinkėjai galėtų dalyvauti rinkimuose, o rinkėjų identifikavimą ir registraciją privalu atlikti teisėtomis priemonėmis. Ši nuostata iš esmės turi įgyvendinti penkias svarbiausias taisykles:

- kiekvienas asmuo, turintis teisę pareikšti savo apsisprendimą, gali tai padaryti;
- galimybė dalyvauti rinkimuose turi būti užtikrinta įstatymiškai;
- balsavimo technologijos ir priemonės turi būti suprantamai paaiškintos rinkėjams ir neturi būti jokių ribojimų susipažinti su technologijomis, panaudotomis rinkimų procese;
- elektroninis balsavimas yra tik papildoma priemonė pagrindinio balsavimo kontekste;
- balsavimui naudojama infrastruktūra turi būti prieinama visiems rinkėjams (Gritzalis, 2002).

Pasirinkimo laisvės principas, užtikrinantis, kad rinkėjas nebuvo verčiamas pasinaudoti elektroninio balsavimo sistema, taip pat nebuvo technologiškai paveiktas pareikšdamas savo nuomonę. Iš esmės užtikrinant ši principą turi būti atsižvelgiama į dar kelis aspektus: balsavimo sistema turi užtikrinti rinkėjui galimybę balsuoti „tuščiu biuleteniu“.

Lygybės principas. Turi būti užtikrinta lygybė rinkimuose dalyvaujančioms partijoms ir kandidatams, taip pat balsavimo teisę turinčių rinkėjų teisių lygybė. Pagrindinis e. balsavimo reikalavimas – popieriniai ir elektroniniai balsavimo biuleteniai turi būti identiški. Įgyvendinant šį principą taip pat privalo būti užtikrinta ir vienoda politinių partijų galimybė stebėti e. balsavimo sistemas ir e. balsavimų eigą. Kai kurie ekspertai e. balsavimo sistemas rekomenduoja įrengti taip, kad e. balsavimas vyktų anksčiau nei „popieriniai“ rinkimai.

Slaptumo principas turi užtikrinti, kad: e. balsai bus slapti visą laiką, kol vyks balsavimas iki galutinio jų skaičiavimo; nė vienas asmuo negalės susieti balsavusio žmogaus ir jo balso; bus aiškiai atskirtos registravimosi balsavimui ir balsavimo fazės; vartotojas jokiomis priemonėmis, kurios yra susietos su balsavimo sistema, negalės pateikti informacijos apie savo pasirinkimą. Būtina pažymėti, kad slaptumo principas turi įgyvendinti ir tai, kad balsavimo sistemoje privalo būti sukonstruota tiksli balsų skaičiavimo ir, jei būtina, perskaičiavimo galimybė, neidentifikuojant balsavusiojo asmenybės (International Working Group for Data Protection, 2001).

Tiesiogiškumo principas nusako būtinybę vykdyti rinkimus taip, kad kiekvienas balsas būtų tiesiogiai įrašytas ir suskaičiuotas. Siekiant neapkrauti e. balsavimo sistemų ir supaprastinti jų veikimą, dažniausiai visi rinkimų proceso metu gauti balsai yra saugomi užkoduoti ir atkoduojami tik rinkimams pasibaigus.

Demokratijos principas. Šiuo principu privaloma užtikrinti e. balsavimo sistemų atitiktį įprastinių tradicinių balsavimo sistemų principams. Savaime suprantama, kad atsiranda tam tikrų specialiųjų reikalavimų, kurie turi būti įgyvendinti elektroninio balsavimo sistemose. Šie reikalavimai apima kuriamų ar sukurtų elektroninio balsavimo sistemų teisėtumą, skaidrumą, saugumą ir tikslumą. E. balsavimo sistemos naudotojai turi suprasti sistemos veikimą, bet tai kartais tiesiog neįmanoma padaryti, kadangi dalis individų neturi informacinėms technologijoms perprasti reikalingų bazinių žinių. Kitaip tariant, pasitikėjimas e. balsavimo sistemomis yra grįstas pasitikėjimu technologijomis ir balsuojančiojo asmens pasiruošimu įsisavinti ir naudoti technologijas.

3. Elektroninių rinkimų sistemų modelių lyginamoji analizė

Elektroninių rinkimų sistemos gali būti skirstomos pagal tai, kiek ciklų privalu užbaigti rinkėjui, norint pareikšti savo valią rinkimuose. Dauguma dabartinių e. rinkimų modelių, šiuo metu egzistuojančių pasaulyje, skirstomi į vienos ir dviejų fazių modelius, kartais vadinamus vieno ir dviejų ciklų modeliais. Taip pat egzistuoja vadinamieji n-fazių (n-ciklų) modeliai, kadangi naudojant juos reikalaujama, jog rinkėjas, pareikšdamas savo valią rinkimuose, atliktų daugiau nei du balsavimo ciklus. Kiekviena balsavimų sistemos fazė numato tam tikrų rinkėjo veiksmų atlikimą konkrečiai nustatytu laiku. Visos fazės eina viena paskui kitą ir negali būti sukeistos vietomis. Elektroninio balsavimo sistemos fazės nebūtinai turi atitikti fazes, kurios yra aprašytos techninėse specifikacijose (angl. *Election Markup Language – EML*). Kai kurios iš šių fazių gali būti vienodos, bet kai kurios balsavimo modelio fazės visinėje sistemoje gali būti sujungtos į

keletą EML fazių. Pvz., elektroninėje balsavimo sistemoje gali būti reikalaujama rinkėjo registracijos ir galimybės atiduoti balsą už jam patinkantį kandidatą dviem skirtingais žingsniais (Prosser et al., 2009). EML požiūriu vartotojo registracija balsavimo sistemoje atitinka pirmą fazę, o pati balsavimo procedūra, vertinant iš elektroninių balsavimų sistemos modelio pozicijos, yra antra fazė. Porinkiminiai uždaviniai, vykstantys sistemoje ir aprašomi EML, nėra nagrinėjami, kadangi jie nėra reikšmingi rinkėjui (Rössler, 2004).

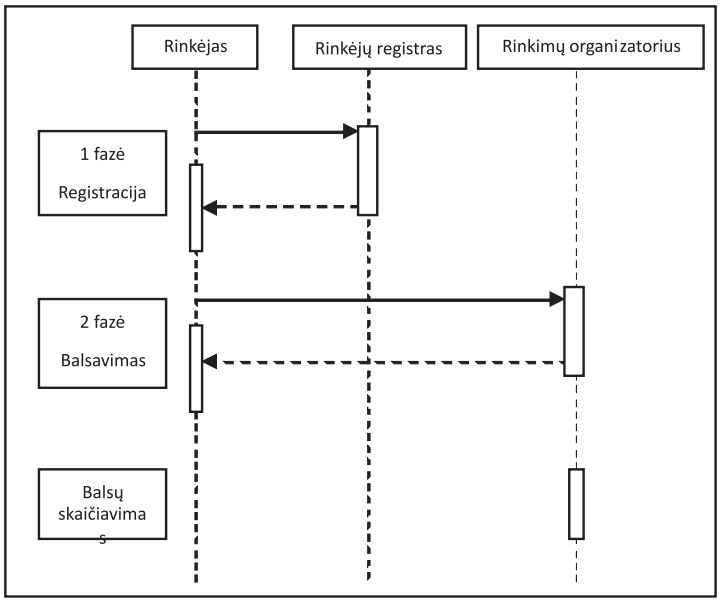
3.1. Vienos fazės modelis

Vienos fazės modeliu grįstos elektroninio balsavimo sistemos yra labai retos. Vienos fazės modelio esmė – rinkėjas, norintis pareikšti savo valią rinkimuose, gali tai atlikti vienu paprastu veiksmu. Taikiant tokius modelius, rinkėjui, prieš balsuojant, nereikia savęs identifikuoti sistemoje elektroninėmis priemonėmis. Žiūrint iš rinkėjo pusės, toks balsavimas vyksta vienu ciklu. Sunkiai įsivaizduojama, kaip galima pritaikyti tokiu modeliu grįstą balsavimo sistemą e. rinkimams, vykdomiems nuotoliniu būdu, kadangi visiškai neįmanoma užtikrinti, kad vartotojas nebalsuos daugiau kaip vieną kartą ir nebus pažeista nuostata, leidžianti elektroninių rinkimų sistema balsuojančiam piliečiui atiduoti balsą tik vieną kartą (Recommendation Rec(2004)11 of the Committee of Ministers). Faktiškai vienos fazės balsavimo sistemos modelis gali būti pritaikomas tik elektroniniams rinkimams, kurie yra vykdomi kontroliuojamoje aplinkoje: rinkimų apylinkėse, balsavimo kioskuose ir kitose vietose, kur yra patikrinama rinkėjo, patenkančio prie balsadėžės, tapatybė. Nors tokia balsavimo sistema ir nėra tobula, ji vis dėlto pranašesnė už tradicinius „popierinius balsavimus“: rinkėjas, atėjęs į balsavimo apylinkę ir nuėjęs į balsavimo vietą, negalėtų sugadinti balsavimo biuletenio ir bet kuriuo atveju turėtų pareikšti savo valią, taip pat jei rinkimų metu perkami balsai, rinkėjai neturi jokio įrodymo „balso pirkėjui“, kad balsavo būtent taip, kaip ir buvo sutarta. Šis e. rinkimų modelis nėra tobulas, bet jis gali būti derinamas ir taikomas kartu su dviejų fazių modeliu (Rössler, 2004).

3.2. Dviejų ir n-fazių modelis

Dauguma pasaulyje naudojamų elektroninių balsavimo sistemų yra grįstos dviejų fazių modeliu. Šis modelis yra pavaizduotas 1 paveiksle. Paprastai pirmoje balsavimų modelio fazėje rinkėjas privalo save identifikuoti balsavimų sistemoje, kuri išduoda jam tam tikrą „leidimą balsuoti“ ir taip rinkėjas įgauna priėjimą prie antros ir pagrindinės modelio fazės – balsavimo (Rössler, 2004).

Kartais tarp pirmosios, registravimosi, ir antrosios, pagrindinės balso atidavimo, fazės elektroninių rinkimų sistema gali reikalauti iš rinkėjo papildomų veiksmų. Vadinamajame n-fazių modelyje balsuojantis asmuo gauna elektroninių rinkimų sistemos pranešimus, kurie reikalauja registruojantis balsavimams identifikuoti save keliose atsakingų institucijų identifikavimo sistemose, tai realizuojant tam tikrais atskirais žingsniais. Taip registravimosi fazė yra padalinama į keletą fazių ir tokia elektroninių balsavimų sistema yra pagrįsta n-fazių modeliu.



1 pav. (Rössler, 2007)

Apibendrinant vienos, dviejų ir n-fazių e. rinkimų sistemų diegimo ypatumus ir įvertinant jų anksčiau nurodytus privalumus ir trūkumus, galima konstatuoti, kad, žvelgiant į rinkimų organizavimo pasaulines tendencijas pakankamai kritiškai, realiai gali būti svarstomos tik elektroninių rinkimų n-fazių modelio diegimo ir įgyvendinimo galimybės.

4. Elektroninių rinkimų saugumo problematika

Kiekviena šalis supranta, kad elektroniniai rinkimai panaikina visas geografines tradicinių rinkimų sistemų ribas. Rinkimų sistemos nėra sutelktos vienoje geografinėje vietovėje, rinkimų apylinkėje ir yra pasiekiamos bet kuriame pasaulio taške. Tai gali ženkliai padidinti elektroninių „atakų“, nukreiptų prieš elektroninio balsavimo sistemas, skaičių. Elektroninių rinkimų sistemos ir jose organizuojami procesai gali būti labai patrauklus taikinys asmenims, užsiimantiems neteisėtomis veikomis. „On-line“ balsavimo sistemos privalo būti patikimos, turi kelti visuomenei pasitikėjimą, kurį suinteresuoti asmenys gali bandyti sugriauti, paversdami elektroninių rinkimų sistemas „baisiąja rinkimų dienos istorija“ (Crown Copyright, 2002, p. 21).

Norint sukurti patikimą ir gerai apsaugotą elektroninio balsavimo sistemą, be jokios abejonės, reikalingas ilgas ir kruopštus daugelio sričių specialistų (informacinių technologijų, kompiuterių saugumo specialistų, informacinių sistemų projektuotojų) darbas ir būtina susilaikyti nuo bet kokių išankstinių prielaidų ir prognozių su spėlionėmis, kas galėtų nutikti, kai bus galutinai sukonfigūruota ir įdiegta elektroninio balsavi-

mo sistema. Nuomonė apie elektroninių balsavimų saugumą yra suformuota remiantis elektroninių balsavimo sistemos konfigūracija, tačiau šie duomenys yra viešai prieinami ir gali būti panaudoti sistemai kompromituoti.

Be to, būtina ir ypač svarbu yra išnalizuoti grėsmes, kylančias elektroninėms balsavimo sistemoms, ir atskleisti galimus elektroninio balsavimo sistemų „užpuolimo“ būdus, kurie gali sukelti visuomenės nepasitikėjimą elektroninėmis balsavimo sistemomis ir sužlugdyti šių sistemų įdiegimą ir naudojimą, vykdant rinkimų procesus.

Anksčiau nurodytos grėsmės gali būti skirstomos pagal šių grėsmių sukėlėjų tipus. Trumpai apibrėžiant tai yra išorinės ir vidinės grėsmės. Visuomet didesnis dėmesys yra skiriamas išoriniams grėsmių sukėlėjams, bet tai nėra pati teisingiausia pozicija, kurios turėtų būti laikomasi, kadangi žymiai lengviau galima pažeisti sistemą iš vidaus. Tokie (vidiniai) įsilaužimai į kompiuterių sistemas, pasak mokslininkų, sudaro apie 80 procentų visų įvykdytų įsilaužimų (Ūselis, 2000), ir tai viso labo tik ta dalis įsilaužimų, kurie buvo aptikti arba paviešinti.

4.1. Vidinės grėsmės

Skiriamos trys pagrindinės galimų potencialių vidinių grėsmių sukėlėjų grupės:

- Pirmoji grupė yra teisėti elektroninių balsavimo sistemų vartotojai. Jie elektroninių rinkimų sistemose gali ieškoti pažeidžiamų arba saugumo spragų ir, turėdami pakankamai techninių žinių bei pakankamą jiems suteiktą suinteresuotų asmenų paskatą, gali pažeisti elektroninio balsavimo sistemas. Dažniausiai šie veiksmai atliekami siekiant finansinės naudos.
- Antrajai grupei priklauso asmenys, kurie gali siekti pasinaudoti privilegijuota elektroninių balsavimo sistemų operatorių (administratorių) padėtimi, kad pasinaudotų pažeidžiamumu elektroninio balsavimo sistemose. Šios grupės atstovai dažniausiai siekia pasinaudoti valstybės tarnautojais arba kitų organizacijų darbuotojais, kurie kuria elektroninio balsavimo sistemas. Tokie darbuotojai gali turėti pakankamai žinių ir prieėjimą prie elektroninių balsavimo sistemų. Šių grėsmių sukėlėjų pagrindiniai motyvai yra gaunama finansinė nauda arba tiesiog asmeninis pasitenkinimas, savęs realizavimas vykdant neteisėtas veikas. Elektroninių balsavimo sistemų operatoriai ir valstybės tarnautojai turi būti morališkai pasiruošę tokiems suinteresuotų piktavalių veiksmams, jeigu jiems pateikiama visa informacija apie saugumo „skyles“.
- Trečioji didelė grupė yra valstybės tarnautojai, kurie turi priėjimą prie elektroninės balsavimo sistemos, bet nėra susiję su elektroninės balsavimų sistemos įgyvendinimu. Šie asmenys gali dalyvauti arba vadovauti vidinėms elektroninės balsavimo sistemos „atakoms“. Motyvai, dėl kurių šie asmenys gali vykdyti neteisėtą veiką, dažniausia būna finansinio pobūdžio arba tiesiog asmeniniai konkrečiai neįvardinami tikslai (Crown Copyright, 2002, p. 22).

4.2. Išorinės grėsmės

- Pavieniai įsilaužėliai, ieškantys, kaip neigiamai paveikti elektronines balsavimo sistemas vien tam, kad gautų asmeninį pasitenkinimą atakuodami valstybės sistemą arba taip protestuojantys prieš vyriausybės vykdomą politiką. Šie asmenys dažniausiai ieško

galimybės prieiti prie duomenų, juos sugadinti arba pavogti dėl asmeninės naudos arba tiesiog neteisėtam paviešinimui.

• Labai nedaug nuo pavienių įsilaužėlių skiriasi kita tikslinė pažeidėjų grupė, t. y. nusikalstamos organizacijos arba pavieniai nusikaltėliai. Šios grupės arba asmenys, pavyzdžiui, informacijos brokeriai, taip pat gali norėti turėti neteisėtą prieigą prie elektroninių balsavimo sistemų, kad pasinaudotų šių sistemų ištekliais asmeniniais tikslais.

• Protestuojančių asmenų grupės arba „hacktivistai“ gali bandyti nukreipti savo veiksmus prieš elektronines balsavimo sistemas su tikslu parodyti priešiškumą šių sistemų panaudojimui balsavimo procesuose siekdami sugadinti šias sistemas arba tam, kad gautų duomenis asmeniniais tikslais arba informacijos, esančios balsavimo sistemose, gadinimui.

• Užsienio žvalgybų tarnybos gali būti suinteresuotos gauti informaciją apie asmenis. Ateityje šią informaciją jos galėtų panaudoti kontržvalgybai arba šnipinėjimui. Šios tarnybos, naudodamos gautą informaciją, galėtų veikti šalies politikos formavimą arba manipuliuoti turima balsavimo informacija, siekdamos daryti įtaką balsavimo rezultatams.

• Teroristinės organizacijos gali būti suinteresuotos informacija apie privačius asmenis, kuri yra saugoma elektroninio balsavimo sistemose. Šios organizacijos, naudodamos turimas žinias, gali būti suinteresuotos, pvz., rengti teroro aktus. Jos taip pat gali tyrinėti elektroninio balsavimo sistemas ir jose balsavimo metu kaupiamą informaciją, kad suprastų, kokios yra balsavimo tendencijos ir, esant reikalui, daryti įtaką balsavimo rezultatams arba trukdyti vydyti sklandų balsavimo procesą.

5. Elektroninio balsavimo sistemų pažeidimų metodai

Atskleidus svarbiausius elektroninių rinkimų problematikos aspektus, tikslinga išanalizuoti dažniausiai pasitaikančius techninių užpuolimų („atakų“) metodus, kuriuos taiko neteisėtomis veikomis užsiimantys asmenys, siekdami sutrikdyti informacinių sistemų funkcionavimą:

• Elektroninio balsavimo sistemų saugumo spragų paieškos testai (angl. *penetration tests*) gali daryti teigiamą įtaką visuomenės nuomonei apie elektroninį balsavimą. Kad jie būtų efektyvūs, reikia tiesiog modifikuoti sistemoje saugomus duomenis ir skelbti viešai apie pasiektus pozityvius rezultatus. Saugumo spragų paieškos testai gali būti panaudoti ne tik per balsavimą, bet ir bet kuriuo metu po balsavimo. Atakas vykdantiems asmenims pakaktų tiesiog atskleisti balsuojančiųjų asmenų autentifikavimo informaciją, kuria jie naudojasi prisijungdami prie elektroninės balsavimo sistemos. Ši informacija gali būti panaudota tam, kad susietų balsuojantį asmenį su jo balsu. Taip pat spragų paieškų testai gali būti panaudoti su tikslu pakeisti oficialių balsavimo svetainių turinį. Pakeistos elektroninių balsavimo svetainių nuorodos gali daryti įtaką duomenų konfidencialumui ir vientisumui skaičiuojant balsus, o dėl to rinkimai, vykdomi elektroninėmis sistemomis, gali būti pripažinti negaliojančiais. Mažai tikėtina, kad individua-

lios vartotojų sistemos (asmeniniai kompiuteriai) bus patrauklus taikinys „atakas“ vykdantiems programišiams (angl. *hacker*). Labiau tikėtina, kad programišiai gali bandyti sugandinti elektroninių balsavimo sistemų tarnybines stotis. Tokiu atveju būtų atvertas priėjimas prie didesnio duomenų kiekio (Crown Copyright, 2002, p. 22).

• Vienas iš atvejų yra galimybė, kad elektroninių balsavimo sistemų tarnybinėse stotyse prieš rinkimus arba jų metu bus įdiegta piktybinė programinė įranga (angl. *Malicious Software*). Tokią programinę įrangą galima įdiegti į tarnybines stotis naudojantis elektroniniu paštu arba išoriniu ryšiu su tarnybine stotimi. Didelis prisijungimų prie elektroninio balsavimo sistemos tarnybinės stoties skaičius gali žymiai padidinti galimybę piktybinei programinei įrangai plisti tarnybinėje stotyje. Tokiu būdu elektroninio balsavimo sistema gali būti sugandinta. Pavyzdžiui, jei būtų įdiegta „Trojos arklio“ (angl. *Trojan Horse*) tipo programa, gali būti pažeistas duomenų konfidencialumas ir / arba vientisumas. Toks duomenų pažeidimas gali paskatinti atitinkamus šalies paregūnus pasinaudoti pagal savo kompetenciją turima teise skelbti rinkimų rezultatų pripažinimą negaliojančiais. Interneto naršyklių ir operacinių sistemų, kuriomis naudojasi elektroninių balsavimo sistemų vartotojai, saugumo spragos gali atverti daugiau agalimybių tarnybinėse stotyse įdiegti piktybinę programinę įrangą. „Ataką“ vykdantis asmuo, naudodamasis piktybine programine įranga, gali sukonfigūruoti ją taip, kad jokios antivirusinės programos jos neaptiks iki tol, kol ji nebus aktyvuota vartotojo kompiuteryje. Tai gali įvykti tiesiog per pačius rinkimus. Pavyzdžiui, „Trojos arklio“ tipo programa gali kompromituoti balsuojančio asmens rinkimuose pareikštą nuomonę, informuojant apie jo pasirinkimą ne tik elektroninio balsavimo sistemos tarnybinę stotį, bet ir trečiąją šalį arba tiesiog pakeisti balsuojančiojo asmens pasirinkimą be jo žinios, prieš siunčiant jį į elektroninio balsavimo sistemos tarnybinę stotį.

• Dar vienas pažeidimas, kuris gali būti didžiausia problema naudojantis elektroninėmis balsavimo sistemomis, yra paslaugų ribojimas (angl. *Denial of Sevice*). Vienu metu daugeliui vartotojų naudojantis elektroninio balsavimo sistema, ji gali tapti laikinai nepasiekiama. Nusikaltėlių „ataka“, taip pat netinkamas vartotojų naudojimasis elektroninio balsavimo sistema gali sukelti jos laikiną nepasiekiamumą, o blogiausiu atveju – nepasiekiamumą per visą balsavimui skirtą laiką. Tokiu atveju balsuojantys asmenys neturėtų galimybės naudotis elektroninio balsavimo sistemos teikiamomis paslaugomis ir dėl atakų, kurios būtų nukreiptos prieš komunikacijų kanalus. Reikia pabrėžti, kad taip pat išlieka galimybė, jog bus atakuojamas vartotojo įrenginys (personalinis kompiuteris). Tokiu atveju balsuojantis asmuo negalės pasinaudoti jam suteikta balsavimo teise.

• DNS (angl. *Domain Name Service*) „atakos“ taip pat gali būti panaudojamos elektroninų balsavimo sistemų kompromitavimui. Nusikaltėliai klastoja DNS įrašus ir gali sukurti netikras elektroninių balsavimo sistemų kopijas. Į šias netikras elektroninų balsavimo sistemų kopijas besikreipiantys suklaidinti rinkėjai netinkamoje vietoje išreiškia savo valią. Šiuo atveju bus ne tik surinkta informacija apie balsuojančius asmenis, bet ir jų balsai nepasieks tikrosios balsavimo sistemos. Vykdant tokio pobūdžio „atakas“, gali būti kompromituojami rinkėjai, tariamai balsuojant arba pasinaudojant

gautais duomenimis gali būti suklastoti rinkėjų balsai, todėl ir šiuo atveju rinkimai gali būti pripažinti negaliojančiais.

• Viena iš socialinės inžinerijos „atakų“ – tam tikro balsavimo būdo propagavimas, pasinaudojant tikslinėmis rinkimų kampanijos akcijomis (pvz., „nebalsavau elektroniniu būdu“). Visuomenei atitinkamai pateikus informaciją apie elektronines balsavimo sistemas ir tiesiog surengus daugelį akcijų, kuriose būtų tvirtinama, kad toks balsavimo būdas yra nesaugus ir gali būti panaudotas tik tam, kad būtų klastojami rinkimų rezultatai, galima sumažinti vartotojų pasitikėjimą šiuo balsavimo būdu. Tuomet nebus pasiektas rezultatas, kurio yra tikimasi diegiant elektroninio balsavimo sistemas (Crown Copyright, 2002, p. 22).

Taigi, kuriant elektroninio balsavimo sistemas, reikėtų didelį dėmesį skirti šių sistemų pažeidžiamumo analizei, taip pat nepamiršti apie atsarginių – besidubliuojančių, sistemų ir ryšio linijų reikalingumą, kadangi galimi atsitiktiniai elektroninio balsavimo sistemos sutrikimai: techninės įrangos gedimai, ryšio linijų gedimai ir kt. Sugedus elektroninio balsavimo sistemai, visos pastangos sklandžiai organizuoti rinkimus gali būti bevaisės, o visuomenės nuomonė apie balsavimo sistemos naudojimą ateityje bus suformuota ir pakeisti ją būtų labai sunku.

Pasaulyje jau yra pasinaudota keletu tokių anksčiau minėtų ir išanalizuotų metodų. Galima paminėti Nyderlandų Karalystės, Jungtinių Amerikos Valstijų įvykius. Nyderlandų Karalystėje 2006 m. spalio mėnesį organizacija „Mes nepasitikime balsavimo kompiuteriais“ (olandiškai *‘Wij vertrouwen stemcomputers niet’*) per nacionalinę televiziją pareiškė, kad jiems pavyko sėkmingai įsibrauti į „Nedap“ balsavimo kompiuterius (SiliconRepublic.com, 2006). Organizacija parodė, kad, atlikus nesudėtingus veiksmus, kurie užtrunka apie 1 minutę, galima pakeisti balsavimo kompiuterio sudėtines dalis (mikroschemas), kurių pakeitimas gali „išmokyti“ kompiuterį nelabai tiksliai įrašinėti balsavimo rezultatus ir net „žaisti šachmatais“. Taip pat ši organizacija parodė, kaip galima iš 20–30 metrų atstumo (The Register, 2006), pasinaudojant radijo bangų skeneriu, įvykdyti aktyviojo elektromagnetinio spinduliavimo (TEMPEST) „ataką“, kurios metu įmanoma nustatyti, kaip balsavo žmogus, ir tuo pačiu sukelti grėsmę balsavimo slaptumui. Balsavimo mašinas iš Nyderlandų Karalystės ketino nupirkti ir Airijos vyriausybė, bet šio sandorio buvo atsisakyta dėl to, kad balsavimo mašinos buvo pripažintos labai nesaugiomis. 2005 metais JAV Kalifornijos valstija parėmė įsibrovimo į kompanijos „Diebold Election System“ balsavimo įrenginį testą (Computerworld, 2005). Harri Hursti, kuris atliko šį testą, įrodė, kad įrenginys yra nesaugus dėl jame panaudotų techninių sprendimų. Vėliau jis pateikė ataskaitą, kurioje aiškiai matoma veiksmų eiga braunantis į šią sistemą. Taip pat ataskaitoje parodyta, kad balsavimo rezultatai priklauso tik nuo to, kaip yra užprogramuotas įrenginys. 2005 metais JAV ir Kanadoje rinkimams buvo naudojami 1297 tokie įrenginiai (Hursti, 2005, p. 31).

Atlikus detalią elektroninių rinkimų sistemų pažeidimų metodų analizę, galima konstatuoti, kad elektroninės balsavimo sistemos gali būti „atakuojamos“ siekiant įvairių tikslų. Nors patobulintos sistemos ir gali būti pripažintos saugiomis, negalima pamiršti, kad ateityje sistemos saugumas vis tiek gali būti pažeistas. Tam tikslui reikėtų periodiškai atlikti sistemos saugumo pažeidžiamumo testus, nes nepažeidžiama sistema

gali būti laikoma tik iki to momento, kol nėra įrodyta priešingai, o pažeidžiamumų aptikimo testai galės apsaugoti nuo įvykių, kurie neigiamai paveiktų žmonių pasitikėjimą elektroninių rinkimų sistemomis.

6. Išvados

Nors elektroninių rinkimų sistemos ir yra plačiai naudojamos skirtingų valstybių dabartiniuose politiniuose procesuose, jos vis dar nėra tobulos. Tikėtina, kad pakankamai sparčiai plintant naujoms technologijoms, gali pasikeisti ir pačios elektroninių rinkimų sistemos bei jų naudojimo tendencijos pasaulyje. Kuriant ir naudojant e. balsavimo (rinkimų) sistemas privalu laikytis tam tikrų reikalavimų bei užtikrinti, kad balsavimo sistemos bei jų veikimo principai būtų prieinami ir suprantami plačiam vartotojų ratui. Kartais dėl tam tikrų kompiuterinių ir techninių žinių stokos e. balsavimo sistemose vykstantys procesai gali būti nesuprantami visuomenei, o tai reiškia, kad bent jau dabartiniu metu arba vertinant ilgesniu laikotarpiu e. balsavimo sistemos gali būti tik pagalbinis mechanizmas įgyvendinant rinkimus, grindžiamus tradicinėmis rinkimų organizavimo formomis.

Kuriant elektroninių rinkimų sistemas būtina didelį dėmesį skirti šių sistemų saugumui, pažeidžiamumų ir grėsmių identifikavimui bei mažinimui. Laiku pritaikyti įsibrovimų į šias sistemas aptikimo testai ir muolatinė ekspertų priežiūra daro įtaką tam, kad sistema būtų laiku atnaujinama ir saugi, o tai, savaime suprantama, gali lemti pasitikėjimą tokio pobūdžio sistemomis. Gyventojų pasitikėjimas elektroninių rinkimų sistemomis reiškia ne ką kita, kaip „nematomą sistemos“ pridėtinę vertę, kurią sunku sukurti ir palaikyti, bet labai lengva prarasti, be to, toks praradimas reikštų visišką sistemos žlugimą.

Literatūra

E-Voting Security Study, Crown Copyright, 2002. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://www.ictparliament.org/CDTunisi/ict_compendium/paesi/uk/uk54.pdf.

Cybervote, An Innovative Cyber Voting System for Internet Terminals and Mobile Phones, 2001. IST-1999-20338. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://www.eucybervote.org/reports.html.

Computerworld, 2005. Žiūrėta 2012 m. rugsėjo 19 d. Prieiga per internetą: http://computerworld.com/governmenttopics/government/itgovernment/story/0,10801,106665,00.html.

Grimm, R., Krimmer, R., Meibner, N., Reinhard, K., Volkamer, M., and Weinand, M. (2006). Security Requirements for Non-political Internet Voting. Electronic Voting 2006, 2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.5 and E-Voting.CC August, 2nd – 4th, Bregenz, Austria, p. 8–23.

Gritzalis, A. D. (2002). Principles and requirments for a secure e-voting. Copenhagen, p. 110–125.

Hursti, H. (2005). The Black Box Report. Security Alert: July 4, 2005 Critical Security Issues with Diebold Optical Scan Design, p. 14–59.

International Working Group For Data Protection in Telecommunications. Common Position on the Use of the Internet in the Conduct of Elections, Vienna, 2001, p. 95–99.

Krimmer, R.,Triessnigs, S., and Volkamer, M. (2007). The Development of Remote E-Voting Around the World: A Review of Roads and Directions, p. 64–91.

Prossera A., Kofler, R., Krimmer, R., and Unger, M. K. Security Assets in E-Voting. Electronic Voting in Europe –Technology, Law, Politics and Society, Workshop of the ESF TED Programme together with GI and OCG July, 7th–9th, Lake of Constance, Austria, 2004, p. 45–138.

Recommendation of the Committee of Ministers to Member States on Legal, Operational and Technical Standards for E-voting, Zurich, 2004, p. 45–138.

Remmert, M. (2004). Towards European Standards on Electronic Voting. Electronic Voting in Europe –Technology, Law, Politics and Society, Workshop of the ESF TED Programme together with GI and OCG July, 7th–9th, Lake of Constance, Austria, p. 37–77.

Rössler, T. (2004). e-Voting. A survey and Introduction. Secure Information Technology Center, Austria, p. 37–77.

Siliconrepublic.Com. 2006. Žiūrėta 2012 m. spalio 12 d. Prieiga per internetą: http://www.siliconrepublic.com/news/news.nv?storyid= single7158.

Ūselis, D. (2000). Kompiuterinių nusikaltimų formos ir rūšys. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://www.sociumas.lt/lit/nr18/PC.asp.

Volkamer, M., and Hutter, D. From Legal Principles to an Internet Voting System. Electronic Voting in Europe –Technology, Law, Politics and Society, Workshop of The ESF TED Programme together with GI and OCG July, 7th–9th, 2004 in Schloß Hofen/Bregenz, Lake of Constance, Austria.

Wij Vertrouwen Stemcomputers Niet. 2009. Žiūrėta 2012 m. spalio 9 d. Prieiga per internetą: http://www.wijvertrouwenstemcomputersniet.nl/English.

Lietuvos Respublikos Seimo 2006 m. lapkričio 16 d. nutarimas Nr. X-912 „Dėl Balsavimo internetu rinkimuose ir referendumuose koncepcijos patvirtinimo“.

MODELS AND PRINCIPLES OF DESIGNING E-VOTING SYSTEMS, ENSURING ITS PROTECTION

Tadas Limba

Mykolas Romeris University, Lithuania, tlimba@mruni.eu

Konstantin Agafonov

Mykolas Romeris University, Lithuania, ka1979@gmail.com

Summary. *All over the world there is one main problem for government organizations in organizing general elections or referendums. The problem is that citizens are very apathetic and their participation in elections and referendums is very low. The elections and referendums, which are based on the traditional election system, use paper ballots which are inconvenient*

for a lot of citizens who have election rights, because it's not very comfortable or possible to reach voting polls on election day. In this case the participation of citizens is very low, because it's not always possible to visit polling stations when the distance to it is quite far or citizens have no time to vote. One of the easiest ways to increase participation of citizens in the country political processes is creation of electronic voting systems that can be used to cast citizen votes both remotely or not. Because of the opinion that e-voting systems will be more convenient for voters and that this will increase voter turnout on elections and referendums, governments of some countries are trying to create and begin to use those systems in their countries' general elections and referendums.

This scientific paper represents the standards and main aspects of creation of e-voting systems, models and the main threats to electronic voting systems. It discusses system attack methods and people who are interested in compromising e-voting systems. Also it analyses the practice of using e-voting systems for elections and referendums in some world countries.

Keywords: *internet, information technologies, information systems, e-voting, e-voting systems, models of e-voting, principles of e-voting system construction, citizens.*