BALSAVIMAS INTERNETU. Geriausios užsienio praktikos ir taikymo Lietuvoje galimybės

Ignas Rubikas
Simonas Valadkevičius
2015 m. sausio mėn.

BALSAVIMAS INTERNETU

Lietuvoje turime keturių tipų rinkimus: Prezidento, Europos Parlamento, Seimo ir savivaldybių tarybų (bei merų). Analogiškos rinkimams procedūros numatytos ir balsuojant referendumuose. Nuo Nepriklausomybės atgavimo Lietuvoje įvyko 20 rinkimų[1] ir 12 referendumų[2], taigi vidutiniškai po ~1,3 visuotinio balsavimo per metus. Balsavimas rinkimuose yra viena svarbiausių demokratijos gyvavimo sąlygų, todėl jo prieinamumas, sudarant visiems piliečiams lygią ir lengvai įgyvendinamą galimybę balsuoti rinkimuose, yra vienas pagrindinių valstybės įsipareigojimų visuomenei.

Viena iš inovatyvių balsavimo formų – balsavimas internetu. Tai vienas iš elektroninio balsavimo tipų, t. y. balsavimo, kurio metu balsai yra perduodami ir (arba) skaičiuojami elektroninėmis sistemomis. Balsavimo internetu metu rinkėjai perduoda savo balsus internetu, naudodami savo asmeninius įrenginius. Šiuo metu balsavimas internetu visuose rinkimuose įteisintas Estijoje, dalinai įteisintas Prancūzijoje, Šveicarijoje, Australijoje, Kanadoje ir JAV. Parengiamuosius darbus arba bandomuosius projektus įgyvendina 48 valstybės (2011 m. duomenimis[3]).

Balsavimas internetu yra aukštos rizikos projektas dėl dviejų priežasčių. Pirma, dėl rinkimų svarbos valstybės gyvenimui egzistuoja stiprūs interesai šį procesą iškreipti atskirų suinteresuotųjų grupių naudai. Antra, pagrindinė demokratinių rinkimų misija – užtikrinti visuomenės *pasitikėjimą*, kad valdžios rinkimai vyko sąžiningai, kas ir sukuria demokratinės valdžios teisėtumą[4]. Tačiau naujovės rinkimų srityje lengvai gali sukelti nepasitikėjimą, todėl dažnai reikalaujama išskirtinio skaidrumo. Išbandant rinkimų naujoves, būtina užtikrinti išsamias ir patikimas saugos priemones, apsaugančias nuo galimo piktnaudžiavimo per rinkimus ir rezultatų iškraipymo, bei aukštą skaidrumo ir viešumo standartą.

Šiame darbe bus trumpai aptartos balsavimo internetu teikiamos naudos, įvardijamos pagrindinės rizikos ir siūlomi galimi sprendimai joms suvaldyti. Bus aptarta Lietuvos padėtis: teisinė bazė, socialinės aplinkybės bei Seime svarstomi teisiniai pasiūlymai, kaip realizuoti balsavimą internetu. Galiausiai bus pasiūlyti ir pagrįsti galimi šiuo metu Seime svarstomų įstatymo projektų papildymai.

---

1 http://www.vrk.lt/pagal-data (2015-01-15 duomenimis)

2 http://www.vrk.lt/ankstesni

3 http://www.e-voting.cc/en/it-elections/world-map/

4 http://en.wikipedia.org/wiki/Legitimacy_%28political%29#Forms_of_legitimate_government

BALSAVIMO INTERNETU NAUDOS

I nauda. Rinkėjų aktyvumas

Rinkėjų aktyvumas dėl balsavimo internetu gali didėti 2,5 – 4%,
jei internetu balsuoja 1/3 visų balsavusiųjų.

Nors daugelis balsavimo internetu kritikų teigia, kad nėra įrodymų, jog balsavimas internetu padidina rinkėjų aktyvumą[5], o kai kurios šalys aiškiai pareiškė, jog nesitiki aktyvumo didėjimo[6], vis dėlto yra pakankamai įrodymų, kad aktyvumas įvedus balsavimą internetu didėja. Estijos atvejo analizė 2005–2014 m. įtikinamai parodė, jog jei 1/3 visų balsavusiųjų rinkimuose nubalsuoja internetu, galima tikėtis 2,5–4 % rinkimų aktyvumo padidėjimo[7].

II nauda. Balsavimo prieinamumas

Balsavimas internetu palengvina galimybes balsuoti užsienyje
gyvenantiems arba keliaujantiems lietuviams bei neįgaliesiems.

Balsavimas internetu būtų itin naudingas užsienio lietuviams, gyvenantiems atokiuose pasaulio kraštuose: daugelyje Azijos šalių, Pietų Amerikoje. Šiose šalyse ambasados ar konsulatai yra itin toli, todėl galimybės fiziškai nuvykti praktiškai nėra, o balsuoti paštu taip pat neįmanoma: kol iš ambasadų ar konsulatų yra išsiunčiami ir atgal parsiunčiami vokai su biuleteniais, rinkimai jau būna pasibaigę[8]. Balsavimas internetu užtikrintų, kad šie rinkėjai galėtų atiduoti savo balsą LR rinkimuose.

Balsavimas internetu suteiktų galimybę akliesiems pirmą kartą balsuoti slaptai, nes dėl balsavimo internetu sistemoje įdiegtų valdymo balsu modulių aklas rinkėjas galėtų balsuoti savarankiškai, be pagalbininkų. Balsavimas internetu taip pat būtų papildomas būdas balsuoti rinkėjams, įprastai balsuojantiems namuose: neįgaliesiems ir senesnio amžiaus žmonėms.

5 http://www.eui.eu/Projects/EUDO-PublicOpinion/Documents/bochslere-voteeui2010.pdf

6 https://www.regjeringen.no/en/dep/kmd/prosjekter/e-vote-trial/news-about-the-e-vote-2011-project/year/2013/BBC-misreports-on-ending-of-Norwegian-internet-voting-pilots/id764809/

7 http://balsavimasinternetu.lt/balsavimo-aktyvumas/

8 Iš asmeninės komunikacijos su Z. Vaigausku, Vyriausiosios rinkimų komisijos pirmininku.

III nauda. Tikslus ir nešališkas balsų skaičiavimas

Stipriai sumažėja žmogiško šališkumo arba klaidų tikimybė, nes balsų skaičiavimo procesas yra automatizuotas pagal viešą algoritmą.

Balsuojant internetu, balsų padavimo ir skaičiavimo procesas būtų centralizuotas, stebimas kompetentingų stebėtojų ir vyktų viešai pagal iš anksto sutartas taisykles. Todėl būtų praktiškai eliminuojama žmogiškos klaidos tikimybė arba tyčinis šališkumas skaičiuojant biuletenius arba iškreipiant jų reikšmę. Balsavimo rezultatus būtų galima iškreipti tik tuo atveju, jei įsilaužėliai iš išorės nulaužtų sistemą (žr. *III rizika*).

IV nauda. Ypač saugus ir patikimas balsavimas (sukūrus visiško patikrinamumo sistemą)

Balsavimas internetu gali būti saugesnis nei dabartinė rinkimų sistema, jei būtų įdiegta visiško patikrinamumo sistema. Kiekvienas rinkėjas galėtų atsekti savo balsą viso balsavimo internetu proceso eigoje.

Visiško patikrinamumo (angl. *end-to-end verification*) sistema reiškia, kad galima patikrinti ir patikimai įsitikinti, kad rinkėjo balsas buvo: atiduotas kaip ketinta, įrašytas kaip atiduotas, suskaičiuotas kaip įrašytas (angl. *cast as intended, recorded as cast, counted as recorded*). Šie trys žingsniai sudaro internetinio balso „kelionės“ grandinę ir, įrodžius kiekvienos grandies integralumą, įrodomas viso proceso integralumas[9].

Pagal Norvegijos pavyzdį sukūrus visiško patikrinamumo sistemą, balsavimo procesas taptų dar skaidresnis ir patikimesnis nei yra šiuo metu. Savo balsą būtų galima patikimai atsekti nuo to momento, kai pabalsuojate, iki jis yra užfiksuojamas galutiniuose rinkimų rezultatuose.[10] Balsavimo slaptumas būtų užtikrinamas naudojant įrodymą be informacijos (angl. *zero-knowledge proof*), kuris leidžia patikrinti, ar balsas nebuvo pakeistas proceso eigoje (nuo pabalsavimo momento iki užfiksavimo galutiniuose rinkimų rezultatuose), neatskleidžiant už ką buvo balsuota.

9 http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1264852

10 Žr. pranešimus: http://csrc.nist.gov/groups/ST/e2evoting/program_E2E.html

V nauda. Didesnis balso slaptumas, palyginti su balsavimu namuose ir paštu

> Balsuojant paštu užsienyje arba namuose, sudaromos sąlygos daryti spaudimą rinkėjui. Balsuojant internetu, šios sąlygos eliminuojamos.

Balsavimas internetu galėtų padidinti slaptumą, palyginti su balsavimu namuose ar paštu užsienyje. Pavyzdžiui, neįgaliesiems ar senesnio amžiaus žmonėms balsuojant namuose, biuletenius nešiojančiam asmeniui sudaromos sąlygos netiesiogiai spausti ar įtikinėti rinkėją. Balsuojant paštu užsienyje, gali įvykti vadinamasis šeimyninis balsavimas.

Balsuodami internetu iš namų, neįgalieji bei senyvo amžiaus žmonės nebeprivalės susidurti su rinkimų biuletenių nešiotojais, o užsienyje gyvenantys piliečiai galės balsuoti pakartotinai, todėl bus išvengta šių grėsmių.

BALSAVIMO INTERNETU RIZIKOS

Šiuo metu techninio saugumo argumentai yra vieni pagrindinių, kuriais remiantis yra kritikuojamas balsavimas internetu[11]. Saugumo klausimas gali būti išskaidomas į šiuos aspektus: privatumas (kriptografija) ir apsauga nuo balsų klastojimo.

Kaip jau minėta, visiškas patikrinamumas (angl. *end-to-end verification*) yra itin aukšto saugumo standartas, kuriuo yra užtikrinama, kad balsas buvo atiduotas kaip ketinta, įrašytas kaip atiduotas bei suskaičiuotas kaip įrašytas. Tokiu atveju yra galimybė įrodyti, jog balsas suskaičiuotas teisingai. Norvegijos balsavimo internetu bandomieji projektai 2011 ir 2013 m. yra *de facto* pasiekę šį saugumo lygį, išskyrus tai, kad balsų skaičiavimo etape patikimumą užtikrino Vyriausioji rinkimų komisija[12].

Toliau pateikiamos balsavimo internetu rizikos ir galimi sprendimo būdai. Ši informacija parengta vadovaujantis Europos Tarybos, OSCE/OHIDR, IFES ir kitų tarptautinių organizacijų analizėmis, taip pat Norvegijos, Estijos, Šveicarijos, Kanados gerąja praktika.

11 https://www.verifiedvoting.org/resources/internet-voting/

12 Iš diskusijų tarp Ch. Bull, Norvegijos balsavimo internetu sistemos techninio ir saugumo vadovo, ir M. Zimnicko, balsavimo internetu skeptiko Lietuvoje. Diskusija vyko konferencijoje „Balsavimas internetu: techniniai iššūkiai ir galimi sprendimai“, 2015 m. sausio 15 d.

Kaip žinoti, ar sistema bus „saugi“?

> Absoliutus saugumas neegzistuoja, todėl esminis klausimas yra tai, koks yra toleruojamas rizikos lygis.

Pasak kibernetinio saugumo specialistų, absoliutus saugumas egzistuoja tik teoriškai: net labiausiai apsaugotose sistemose visada išlieka klaidos ir įsilaužimo tikimybė, kurios neįmanoma eliminuoti[13]

Tai lemia, kad rizika yra neišvengiama darant bet kokį sprendimą. Vietoj to, vertinamas rizikos laipsnis – kokio dydžio yra įsilaužimo tikimybė, kokie ištekliai reikalingi norint tokį įsilaužimą įgyvendinti ir t. t.[14], o sprendimą lemia naudų ir rizikų balansas bei sprendimų darytojo rizikos tolerancijos lygis.

Estijos atvejis laikomas didelės rizikos projektu: nors pagrindinės rizikos yra suvaldytos, periodiškai pasirodo informacijos apie paliktas saugumo spragas bei architektūrines sistemos silpnybes[15]. Atsakingųjų institucijų ir pareigūnų sprendimas Estijoje buvo prisiimti šias rizikas.

Norvegijos balsavimo internetu sistema buvo ruošta ilgesnį laiką, nustatyti ir pasiekti itin aukšti skaidrumo ir kokybės standartai[16] (pvz., minėtas visiškas patikrinamumas), todėl liekamoji rizika (angl. *residual risk*) yra mažesnė[17]. Net turėdama mažesnį rizikos tolerancijos lygį, Norvegija galėjo įgyvendinti balsavimo internetu sistemą saugiai ir patikimai.

Atskirų valstybių elgesys priklauso nuo toje šalyje pripažįstamo rizikos tolerancijos lygio[18]. Įvedant balsavimą internetu Lietuvoje, sprendimų darytojų ir atsakingųjų institucijų prisiimama rizika priklausys nuo to, kaip konkrečiai bus įgyvendinta sistema: kokie parametrai ir protokolai bus nustatyti, kaip jie bus įgyvendinami, kokios bus tiekėjų ir atsakingųjų institucijų kompetencijos. Turint šią informaciją, bus galima spręsti, ar verta prisiimti šią liekamąją riziką (t. y. ar gaunamos naudos viršija galimas rizikas), ir kaip ja turi būti pasidalyta tarp institucijų.

13 http://www.iso27001standard.com/blog/2012/02/13/why-is-residual-risk-so-important/ , http://kauno.diena.lt/naujienos/lietuva/salies-pulsas/specialistai-kibernetinio-saugumo-centras-negarantuos-absoliutaus-saugumo-649475#.VL-r7WM0P8F

14 http://www.iso27001standard.com/blog/2011/11/22/iso-27001-risk-assessment-treatment-6-basic-steps/

15 https://estoniaevoting.org/ , http://www.osce.org/odihr/77557

16 http://www.osce.org/odihr/elections/109503

17 http://www.iso27001standard.com/blog/2012/02/13/why-is-residual-risk-so-important/

18 http://pmtips.net/defining-risk-management-part-5-risk-tolerance/

I rizika. Balsų klastojimas

Ši rizika apibūdina situaciją, kai internetu atiduotas balsas rinkėjui nežinant yra pakeičiamas ir galutiniuose rinkimų rezultatuose skaičiuojamas kitaip, nei rinkėjas ketino. Ši rizika analizuojama pagal tris balsavimo internetu etapus: balso padavimo, saugojimo ir skaičiavimo.

1. *Rinkėjo kompiuteris: signalo perdavimas į serverį*

Sudarius galimybę pasitikrinti atiduotą balsą, yra užtikrinama, kad atiduotas balsas nebuvo pakeistas kompiuteryje arba perduodant signalą į serverį.

Kadangi dauguma namų ar darbo kompiuterių yra apkrėsti programiniais virusais, yra tikimybė, kad bus įdiegta ir kenkėjiška programa, balsuojanti už kitą kandidatą. Šią riziką galima išspręsti naudojant balso patikrinamumo funkciją, kuri leidžia rinkėjui įsitikinti, naudojant papildomą įrenginį, kad balsas nukeliavo į skaičiavimo serverį nepakeistas.

Estija nuo 2015 m. parlamento rinkimų įsivedė balso patikrinamumo mechanizmą[19], pagal kurį balsas nepriklausomai patvirtinamas dviejų atskirų įrenginių. Nubalsavus per kompiuterį, jame iš karto sugeneruojamas QR kodas, kurį nuskenavus išmaniuoju telefonu iš VRK *serverio* atkeliauja signalas apie tai, koks balsas iš šio kompiuterio buvo užfiksuotas. Yra maža tikimybė, kad tuo pačiu virusu bus apkrėsti abu įrenginiai, todėl bent vienas įrenginys parodytų neatitikimą tarp atiduoto ir užfiksuoto balso. Apie tokius atveju būtų pranešama VRK, kuri fiksuotų pažeidimą ir imtųsi atitinkamų priemonių sukontroliuoti programinį virusą arba neįskaityti pažeistų balsų.

2. Balsų laikymo serveris

Laikant balsavimo duomenų kopijas keliuose serveriuose, balsų suklastojimas viename iš serverių bus aptinkamas kituose serveriuose.

Yra rizika, kad gali būti pakeisti duomenys balsų saugojimo serveryje. Pakeitimai gali būti atliekami tiek iš serverio vidaus (administratorių iniciatyva), tiek iš išorės, įsilaužimo būdu.

Tačiau balsavimo internetu sistema naudos tik saugų elektroninį parašą rinkėjams identifikuoti, todėl balsai liks užšifruoti ir jų pakeisti bus neįmanoma iki to momento, kai jie bus atskirti nuo rinkėjų tapatybės.

Šią riziką galima išspręsti duomenis apie atiduotus balsus laikant keliuose skirtinguose nuotoliniuose serveriuose, kurie tarpusavyje sinchronizuotųsi. Atsiradus nepaaiškinamam neatitikimui viename iš šių serverių, tai rodytų, kad į šį serverį buvo įsilaužta, ir jo duomenys galėtų būti anuliuojami. Todėl norėdami suklastoti balsavimo duomenis, programišiai turėtų

19 http://www.vvk.ee/voting-methods-in-estonia/

įsilaužti į beveik visus serverius, kuriuose laikomi rinkimų duomenys, ir padaryti analogiškus pokyčius, kad nebūtų aptinkamas duomenų neatitikimas. Tai padaryti yra labai maža tikimybė.

3. Balsų skaičiavimo serveris

Balsų skaičiavimą gali atlikti keli serveriai, o taip pat bet kuris rinkėjas.

Įsilaužus į balsų skaičiavimo serverį, atsiranda galimybė pakeisti balsus, nes ten jie jau yra iššifruoti. Šią riziką taip pat galima išspręsti kopijuojant duomenis į kelis serverius (žr. aukščiau). Antras sprendimas, didinantis rinkėjų pasitikėjimą balsavimo internetu sistema, yra suteikti galimybę bet kuriam rinkėjui atsisiųsti visus iššifruotus rinkimų duomenis (be rinkėjų tapatybių) iš balsų laikymo serverio. Rinkėjai galėtų patys įsidiegti viešai prieinamą balsų skaičiavimo algoritmą ir, atlikę skaičiavimą savo įrenginyje, sutikrinti gautus rinkimų rezultatus su paskelbtaisiais.

II rizika. Balsų išslaptinimas (techninis pjūvis)

Internetu paduoti balsai yra užšifruojami, o jų išslaptinimas užtruktų ne vieną tūkstantį metų.

Slaptas balsavimas yra viena pagrindinių rinkimų teisių ir kartu esminis reikalavimas, keliamas balsavimo internetu sistemai. Perduodant, saugant ir skaičiuojant duomenis kyla rizika, kad bus atskleista rinkėjo tapatybė. Pagrindinė balsų išslaptinimo rizika yra tai, kad balsavimo internetu duomenys gali būti pavogti ir atskleistos su biuletenyje užfiksuotais pasirinkimais susijusios rinkėjų tapatybės. Tačiau šiandien jau egzistuoja kriptografiniai algoritmai, galintys užtikrinti rinkėjo balso slaptumą pakankamai ilgai po rinkimų – nuo 30 metų (Estija)[20] iki 10 tūkst. metų[21].

Būsimuose įstatymo įgyvendinamuosiuose aktuose būtina numatyti aiškius duomenų perdavimo, apdorojimo ir skaičiavimo protokolus bei standartus, paremtus standartizuotais ir išbandytais konceptais. Pateikus aiškius ir pripažintus saugumo reikalavimus programinės įrangos tiekėjui, galima sukurti balsavimo internetu sistemą, kuri nepažeistų konstitucinės teisės į slaptą balsavimą iš techninės pusės, t. y. būtų neįmanoma atskleisti rinkėjo tapatybės.

20 Iš Arnio Paršovo, Tartu universiteto doktorantūros studento, pristatymo. Pristatymas vyko konferencijoje „Balsavimas internetu: techniniai iššūkiai ir galimi sprendimai“, 2015 m. sausio 15 d.

21 SHA-256 kriptografinė funkcija, pakartota 5–10 tūkst. kartų naudojant dabartinius superkompiuterius, yra iššifruojama per 10 tūkst. metų.

III rizika. Balsavimo slaptumo pažeidimas (socialinis pjūvis), papirkinėjimas

Pakartotinis balsavimas nesudaro galimybių tretiesiems asmenims žinoti, ar jiems pateiktas biuletenis yra tikras, t. y. paskutinis.

Viena iš pagrindinių socialinių rizikų, susijusių su balsavimu internetu, yra balsų papirkinėjimas ir balso paviešinimas artimoje socialinėje aplinkoje. Iš visų nuotolinio balsavimo metodų balsavimas internetu teigiamai išsiskiria, nes yra suvaldoma papirkinėjimo ir balsavimo slaptumo pažeidimo rizika. Šiuo metu Lietuvai yra siūloma įdiegti balsavimą internetu, kuriame kiekvienas rinkėjas galėtų balsuoti pakartotinai neribotą skaičių kartų.

Pakartotinis balsavimas užtikrina balso slaptumą, leisdamas tai daryti slaptai ir atsispirti prievartai, jei balsuoti nori priversti, pavyzdžiui, šeimos narys arba darbdavys. Balsuojant internetu, darbdaviui ar šeimos nariui matant galima žymėti biuletenius ar pateikti įrodymus, bet niekas, išskyrus patį rinkėją, negalės užtikrintai žinoti, kuris iš tų biuletenių yra paskutinis, t. y. tikrasis. Jei rinkėjas yra motyvuotas pakeisti susiklosčiusią situaciją, sukliudyti nubalsuoti iš naujo yra sunku. Be to, pasibaigus balsavimui internetu rinkėjas gali nubalsuoti apylinkėje ir taip anuliuoti anksčiau internetu atiduotą balsą. Tokia sistema jau pasiteisino Estijoje.

Kita vertus, išlieka rizika, kad rinkėjui daromas spaudimas arba vykdomas balso pirkimas baigiantis balsavimo internetu laikotarpiui. Tokiu atveju rinkėjas nespėtų nubalsuoti iš naujo internetu ir galėtų tai padaryti tik apylinkėje.

IV rizika. Įgyvendintojų kompetencijų trūkumas

Įgyvendinančių institucijų darbo kokybę užtikrintų adekvatūs žmogiškieji ištekliai, atsižvelgimas į gerąsias užsienio šalių praktikas ir ekspertų rekomendacijas bei laipsniškas projekto įgyvendinimas.

Ligšiolinė valstybinių IT projektų patirtis rodo skaidrumo, patikimumo ir kokybės trūkumą[22] ir kelia abejonių dėl pakankamos institucijų kompetencijos projektui įgyvendinti. Balsavimo internetu skeptikai Lietuvoje nuosekliai teigia[23], jog ligšiolinė valstybinių institucijų darbo kokybė balsavimo internetu srityje yra nepatenkinama.

Balsavimo internetu projekto valdymas yra kompleksinis ir sudėtingas. Todėl įgyvendinančioji institucija privalo turėti žmogiškųjų bei finansinių išteklių įgyvendinti visoms

22 Pavyzdžiui: http://www.veidas.lt/valstybiniu-misku-svetaine-verta-milijonu-ar-tik-keliasdesimties-tukstanciu arba http://iq.lt/lietuva/e-demokratija-islaidu-daug-naudos-nematyti

23 https://www.facebook.com/groups/269824520243/?fref=ts

susijusioms veikloms, kurių yra daugiau nei vienkartinis viešojo pirkimo atlikimas – tai taip pat gebėjimas savarankiškai kurti ir koreguoti balsavimo internetu protokolą ir procedūras, vykdyti nuolatinį ir nepriklausomą IT vertinimą bei priežiūrą, rinkėjų švietimas. Įvertinti šiuos aspektus privalo pati VRK arba jos paskirta ilgalaikė projekto įgyvendinimo komanda, prisiimanti atsakomybę už projektą. Dėl to būtina kelti VRK darbuotojų gebėjimus šioje srityje ir (arba) numatyti griežtesnį reglamentavimą, įstatymu įpareigojant instituciją įgyvendinti įvairiapusiškas kontrolės ir saugumo užtikrinimo priemones.

Rekomenduojama įgyvendinti projektą pagal išbandytus ir viešai pripažintus standartus. Antra, ruošiant būsimos sistemos parametrus ir reikalavimus tiekėjams bei tvarkos aprašus įgyvendinančioms institucijoms, vadovautis tarptautinių organizacijų parengtomis analizėmis ir ataskaitomis. Rekomenduojama išsamiai konsultuotis su nuo tiekėjų *nepriklausomais*, balsavimo internetu projektų įgyvendinimo srityje patirties turinčiais ekspertais. Be to, rekomenduojama vykdyti simuliacijas, siekiant išbandyti realistinį prototipą praktikoje prieš naudojant jį rinkimuose.

Siūloma projektą įgyvendinti laipsniškai, pirmą kartą leidžiant balsuoti internetu per 2019 m. savivaldybių tarybų arba Europos Parlamento rinkimus. Iki 2016 m. Seimo rinkimų, jei nenorima skubėti, nebus spėta paruošti kokybiškų įstatymo įgyvendinamųjų aktų, įvykdyti viešųjų pirkimų, sukurti Lietuvos reikalavimus atitinkančios balsavimo internetu sistemos.

V rizika. Visuomenės nepasitikėjimas ir kokybės kontrolė

Projekto sėkmę ypatingai lemia visuomenės pasitikėjimas. Jį galima sukurti diegiant patikimas skaidrumo ir viešumo priemones.

Kaip rašoma Europos Tarybos (ET) ataskaitoje (2010)[24], pastaraisiais metais akivaizdžiai paaiškėjo, kad elektroninio balsavimo sistemos negali būti diegiamos, kol nėra pasitikėjimo esamomis rinkimų sistemomis. Visuomenės nepasitikėjimas yra viena pagrindinių priežasčių, kodėl pasaulio šalims nepasiseka balsavimo internetu projektai. Dažnai visuomenės nepasitikėjimą skatina tai, kad keli žinomi IT ekspertai (pavyzdžiui, B. Simons[25]) nepritaria balsavimui internetu, arba tai, kad daug šalių išbandė šį balsavimo būdą ir jo atsisakė[26].

Svarbiausios priežastys, lemiančios visuomenės nepasitikėjimą, yra dvi:

1) kokybiškos ir saugios balsavimo internetu sistemos nebuvimas ir (arba)

24 ET ataskaita, įžanga. Prieiga per internetą: https://book.coe.int/usd/en/constitutional-law/4516-e-voting-handbook-key-steps-in-the-implementation-of-e-enabled-elections.html

25 https://www.youtube.com/watch?v=Wv3VuGZzdK8

26 http://www.delfi.lt/verslas/verslas/i-rubikas-balsavimas-internetu-ar-tikrai-nepasiruose.d?id=66350476

2) tinkamos informacijos apie šią sistemą trūkumas.

Pirmajai problemai išspręsti yra skirtos techninio ir operatyvinio saugumo bei kokybės užtikrinimo priemonės, išvardytos *I–IV rizikų* punktuose. Kalbant apie antrąją problemą, reikėtų užtikrinti, kad esminė informacija apie sistemos veikimą būtų viešai prieinama ir suprantama visuomenei. Būtent į tai yra orientuoti siūlomi sprendimai, visapusiškai atskleidžiantys sistemos veikimo principus ir mechanizmus: viešas ir išsamus auditas, atviras programos kodas ir atvirasis protokolas, balso patikrinamumas ir rinkimų stebėsena.

1. Išsamus auditas

Audito metu išsamiai patikrinama sistema, o išvada pateikiama viešai.

Vienas galimų sprendimų yra išsamus ir viešas balsavimo internetu sistemos auditas, atliekamas prieš ir per kiekvieną balsavimą bei po jo (ET, 2004[27]). ET ataskaitoje (2010) taip pat rekomenduojama, jog audito ataskaita būtų pateikiama specialių žinių nereikalaujančia kalba[28]. Visa tai leistų rinkėjams įsitikinti, kad balsavimo internetu sistema buvo visapusiškai patikrinta nepriklausomų kompetentingų auditorių, ir sumažintų vadinamąjį juodosios dėžės efektą bei iš to kylantį nepasitikėjimą.

2. Atviras programos kodas ir atvirasis protokolas

Programinio kodo ir protokolo paviešinimas leidžia kiekvienam norinčiam įsitikinti sistemos saugumu.

Turi būti pateikiamas viešas programinis kodas bei balsavimo internetu sistemos protokolas, t. y. procedūros, procesai, veikimo schemos, elgesio modeliai skirtingomis situacijomis ir t. t.[29] Šios dvi dalys lemia svarbiausias su techniniu ir operatyviniu saugumu susijusias rizikas. Pagal naudojamą programinį kodą veikia balsų perdavimo, saugojimo ir skaičiavimo mechanizmai. O naudojamas protokolas nusako tai, kaip elgiasi žmonės, administruojantys ir kitaip susiję su sistema. Šių dalių paviešinimas gali padidinti visuomenės pasitikėjimą ir užkirsti kelią netinkamai arba aplaidžiai sukurtai sistemai[30].

3. Rinkimų stebėsena

Balsų skaičiavimo metu stebėtojai užtikrintų, kad viskas vykdoma pagal numatytą tvarką. Taip būtų užtikrinamas proceso patikimumas.

27 ET ataskaita, p. 99–110. Prieiga per internetą: https://wcd.coe.int/ViewDoc.jsp?id=778189

28 ET ataskaita, 5.1.1. punktas. Prieiga per internetą: https://book.coe.int/usd/en/constitutional-law/4516-e-voting-handbook-key-steps-in-the-implementation-of-e-enabled-elections.html

29 http://balsavimasinternetu.lt/protokolas/

30 https://estoniaevoting.org/findings/summary/

Balsavimas internetu dažnai kritikuojamas dėl „juodos dėžės sindromo“. Tai reiškia, kad sunku ar net neįmanoma žinoti, kaip veikia sistema, ir tai kelia nepasitikėjimą. Tačiau tai netiesa: sukūrus tinkamas sąlygas, stebėtojai gali dalyvauti rinkimų internetu stebėsenoje panašiomis sąlygomis, kaip ir balsuojant apylinkėse. Būtina užtikrinti prieigą plačiam stebėtojų ratui. Jei rinkimus stebėtų pakankamas kiekis šios srities ekspertų, kurie pateiktų savo išvadas, tai padėtų sukurti konsensusą visuomenėje dėl balsavimo internetu sistemos vertinimo, kuris galėtų būti atsakas į bandymus kelti nepasitikėjimą. Vidiniai šalies ir tarptautiniai stebėtojai (pvz., OSCE/ODIHR) turėtų gauti didžiausią įmanomą prieigą, kad galėtų stebėti, kaip paruoštas programinis kodas, kaip įgyvendinamas balsavimo internetu protokolas: balsavimo procesas, schemos, saugos reikalavimai, veiksmų planai ir t. t.[31]

31 ET ataskaita, 2.2.1 punktas. Prieiga per internetą: https://book.coe.int/usd/en/constitutional-law/4516-e-voting-handbook-key-steps-in-the-implementation-of-e-enabled-elections.html

BALSAVIMAS INTERNETU LIETUVOJE

2006 m. Seimas patvirtino balsavimo internetu koncepciją. 2009, 2010 ir 2011 m. Seimas balsavo dėl šį rinkimų būdą įteisinančių įstatymo projektų ir visus juos atmetė. 2014 m. lapkričio 6 d. Seimas pateikimo stadijoje pritarė (50 „už“, 13 „prieš“, 31 susilaikė) įstatymo projektams XIIP-1835, 1836, 1837, 1838, 1839[32] ir atidėjo tolesnį projekto svarstymą pavasario sesijai.

Numatomi parametrai

Šiuo metu svarstomame įstatyme numatyti keli būsimos sistemos parametrai:

1. Balsavimas internetu vyksta iš VRK svetainės, ir duomenys kaupiami bei apdorojami VRK valdomoje sistemoje.
2. Balsavimas internetu yra išankstinis, t. y. prasideda šešios dienos prieš balsavimo apylinkėse pradžią ir baigiasi tris dienos prieš tai.
3. Balsuoti internetu rinkėjai gali pakartotinai (įskaičiuojamas paskutinis balsas), taip pat nubalsavę internetu gali balsuoti kitais būdais.
4. Balsuojantys internetu rinkėjai savo tapatybę nustato elektroniniu būdu.
5. Visa kita savo tvarkos aprašu nustato VRK.

Įvertinimas ir identifikuotos problemos

1. Įstatymo projektuose yra įtvirtintas tik pats balsavimo internetu įteisinimo faktas ir kai kurios bazinės procedūros, likęs reglamentavimas paliktas nustatyti VRK tvarkos aprašu, kuris nėra pateikiamas su įstatymo projektu viešai diskutuoti, todėl nežinoma, kokia balsavimo internetu sistema kuriama. Tai kelia visuomenės bei politikų nepasitikėjimą.

2. Trūksta nuostatų, užtikrinančių projekto skaidrumą. Vienintelė numatyta priežiūra yra auditas pagal Valstybės informacinių išteklių valdymo įstatymą[33] „ne rečiau nei kartą per trejus metus“. Taip pat nėra nuostatų, kad sistemos programos kodas bei protokolas būtų viešas. Nenumatomos stebėtojų vaidmenys ir teisės stebint sistemos veikimą.

3. Nenumatomos papildomos saugumo ir pasitikėjimo užtikrinimo priemonės, pavyzdžiui, galimybė patikrinti balsą ar visiškas patikrinamumas.

32 http://www3.lrs.lt/pls/inter/w5_sale.bals?p_bals_id=-19203

33 http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=442491

4. Projektą planuojama įgyvendinti skubiai, o tai neužtikrina saugumo ir kokybės standartų.

IŠVADOS IR PASIŪLYMAI LIETUVAI

Apibendrinant balsavimo internetu projekto galimybes Lietuvoje, daromos išvados[34]:

1. Dabartinė rinkimų sistema yra tobulintina, todėl įvedus balsavimą internetu LR piliečiai iš to gautų naudos.

2. Balsavimo internetu projektas yra rizikingas ir kompleksiškas, tačiau rizikos iš principo yra išsprendžiamos ir tarptautiniai tiekėjai gali pasiūlyti sprendimus, jei bus numatyti aiškūs reikalavimai. Tai priklausys nuo politikų, visuomenės ir įgyvendinančiųjų institucijų suvokimo apie rizikas ir nusiteikimo jas spręsti.

3. Kol kas sistemos skaidrumo standartai nėra patenkinami projekto įgyvendinimui Lietuvoje. Todėl šioje studijoje rekomenduojami balsavimo internetu įstatymo projekto patobulinimai, užtikrinantys skaidrumą: auditas, atviras programos kodas bei atvirasis protokolas, balso patikrinamumas ir rinkimų stebėsena.

4. Teisinis reglamentavimas yra numatytas, tačiau balsavimo internetu veikimo principai nėra įvardyti pakankamai konkrečiai, kad būtų įmanoma vertinti būsimos sistemos saugumą ir patikimumą. Siekiant sudaryti galimybę tai vertinti, reikalingi parametrai, nustatomi įstatymu, VRK tvarkos aprašu ir technine specifikacija.

Pasiūlymai įstatymo projektų papildymui pateikiami priede.

34 Parengta laikantis vertinimo struktūros, pasiūlytos: B. Goldsmith, *Electronic Voting & Counting Technologies: A Guide to Conducting Feasibility Studies*, 2011, p. 31–44. Prieiga per internetą: http://www.ifes.org/Content/Publications/Books/2011/Electronic-Voting-and-Counting-Technologies-A-Guide-to-Conducting-Feasibility-Studies.aspx.