„Atviras Kodas Lietuvai“ valdybos nario, Lietuvos kompiuterininkų sąjungos Kibernetinės saugos sekcijos nario, programuotojo Manto Zimnicko pastabos įstatymo projektui 15-4832(4). Tel.: +370 670 15 171
Data: 2015-12-11. Originalą galima rasti adresu https://gist.github.com/sirex/92219346bff51f9583b7

Pastabų santrauka

1. Prieš įteisinant didelio masto balsavimą nekontroliuojamoje aplinkoje turi būti atliktas socialinis tyrimas dėl balsų papirkinėjimo, įtakos darymo ir požiūrio į galimybę pasinaudoti pakartotinio balsavimo galimybe.
2. Būtina ne tik suteikti galimybę pasitikrinti ar balsas buvo įskaitytas ir suskaičiuotas, bet taip pat būtina užtikrinti, kad visi internetu balsavę pasinaudojo tokia galimybe. Priešingu atveju, už rinkėją gali nubalsuoti virusas.
3. Įstatyme nėra apibrėžta, kas yra stebėtojas. Būtina užtikrinti, kad balsavimo internetu stebėtojų būtų ne mažiau, nei įprastinio balsavimo rinkimų dieną. Interneto technologija iš esmės suteikia galimybę visiems rinkėjams būti stebėtojais. Kuo daugiau stebėtojų, tuo didesnis pasitikėjimas balsavimu internetu.
4. Tiesioginis balsavimo internetu stebėjimas yra neįmanomas. Atliekant stebėjimą naudojantis vieno tiekėjo programine įranga, stebėjimas netenka prasmės. Kiekvienas stebėtojas turi turėti galimybę pasirinkti stebėjimo priemones iš skirtingų tiekėjų. Kad tai būtų įmanoma, visos techninės detalės apie naudojamus protokolus, formatus ir algoritmus turi būti pateiktos viešai ir prieinamai.
5. 13-ame straipsnyje nurodyta, kad balsadėžėje biuleteniai saugomi kartu su rinkėjo tapatybės duomenimis ir tik pasibaigus rinkimų dienai biuleteniai atskiriami nuo tapatybės duomenų. Tai iš esmės prieštarauja konstituciniam slapto balsavimo principui ir šio įstatymo 3-ečio straipsnio aprašytiems slaptumo užtikrinimo principams.
6. 14-ame straipsnyje matyti kokiu tikslu saugomi rinkėjo tapatybės duomenys, tam, kad būtų galima ištrinti internetinį biuletenį, jei rinkėjas ateina balsuoti rinkimų dieną į apylinkę. Tačiau tai iš esmės prieštarauja slaptumo užtikrinimui ir balsadėžės vientisumo išlaikymui.
7. 15-ame straipsnyje nurodyta, kad balsadėžė bus sunaikinama. Sunaikinus balsadėžę neliks jokių įrodymų apie tai ar balsai buvo suskaičiuoti teisingai. Norint įsitikinti ar balsas buvo įskaitytas ir suskaičiuotas teisingai, kiekvienas rinkėjas pasibaigus rinkimams turi turėti galimybė atsisiųsti visą balsadėžę ir kriptografinių algoritmų pagalba įsitikinti ar jo balsas buvo įskaitytas ir suskaičiuotas teisingas, ir ar balsadėžės vientisumas nebuvo pažeistas.
8. 15-ame straipsnyje, 6-ame paragrafe teigiama, kad balsavimo internetu informacinė sistema bus uždaro kodo ir norint susipažinti su sistemos kodu būtina pasirašyti konfidencialumo sutartį. Toks apribojimas kelia nepasitikėjimą sistema, kadangi net jei sistemoje bus surasta saugumo spragų, apie jas gali niekas nesužinoti. Tiek Estijos, tiek Norvegijos balsavimo internetu sistemos yra atviro kodo. Uždaras kodas taip pat parodo, kad balsavimas internetu bus įmanomas naudojantis tik vieno tiekėjo programine įranga, kas taip pat kelia nepasitikėjimą.
9. 18-ame straipsnyje siūloma iš karto imtis sistemos įgyvendinimo. Balsavimo internetu sistema nėra eilinis IT projektas, todėl jos kūrimui negali būti taikomi eilinių IT projektų kūrimo principai. Prieš pradedant įgyvendinimą būtina viešai paskelbti pasirinkto balsavimo internetu protokolo detalų techninį aprašymą. Pilnai suderinus protokolą ir gavus pritarimą iš nepriklausomų ekspertų, protokolas turi būti pridedamas kaip įstatymo priedas ir nekeičiamas. Patvirtinto protokolo pagrindu galima imtis sistemos įgyvendinimo ir tai gali daryti daugelis tiekėjų, kad rinkėjai turėtų platesnį pasirinkimą su pritaikymu įvairiems įrenginiams ar naudojamoms platformoms.

Pastabos dėl balsavimo internetu sistemos

Nuoroda į cituojamą įstatymo projektą 15-4832(4):

http://www.lrs.lt/pls/proj/dokpaieska.showdoc_l?p_id=1099603&p_org=8&p_fix=y

Žemiau cituojamos įstatymo dalys ir po kiekviena citata pateiktos pastabos.

2 straipsnis. Pagrindinės šio įstatymo sąvokos

[...]

3. Balsavimas nekontroliuojamoje aplinkoje – balsavimas iš anksto internetu akivaizdžiai nedalyvaujant rinkimų komisijų nariams.

Prieš įteisinant balsavimą internetu ir reguliariais intervalais turi būti atliekamas socialinis tyrimas dėl balsavimo nekontroliuojamoje aplinkoje.

Balsuoti nekontroliuojamoje aplinkoje turi būti leidžiama tik tokiu atveju, jei socialinio tyrimo rezultatai yra teigiami. Teigiamas rezultatas reiškia, kad pakankamai mažas skaičius žmonių, balsuodami nekontroliuojamoje aplinkoje, gali patirti įtaką, spaudimą ar tiesiog sutiktų parduoti savo balsą.

Atliekant tokį tyrimą reikėtų išsiaiškinti, kiek žmonių pardavę balsą arba patyrę įtaką, pasinaudotų pakartotinio balsavimo galimybe.

Taip pat būtina pastebėti, kad priklausomai nuo pasirinkto balsavimo internetu protokolo, pakartotinio balsavimo galimybė neužtikrina apsaugos nuo balsų papirkinėjimo ar įtakos darymo. Pavyzdžiui, pasirinkus variantą, kuriame rinkėjas gauna įrodymą, kurio pagalba gali anuliuoti savo balsą arba įsitikinti, kad balsas buvo įskaitytas ir suskaičiuotas teisingai. Tokio įrodymo gali pareikalauti papirkinėtojas, kuris bus garantuotas savo pirkiniu.

Beje, įrodymo turėjimas yra vienintelė žinoma priemonė, kuri užtikrina 12-ame straipsnyje aprašytus balso patikrinimo principus.

12 straipsnis. Rinkėjo balso patikrinimo principai

[...]

1. balsuota kaip norėta: tai principas, kuris leidžia rinkimų laikotarpiu rinkėjui įsitikinti, kad užkoduotas balsas yra toks, kokį rinkėjas norėjo pateikti;
2. įrašyta kaip pateikta: tai principas, kuris leidžia rinkimų laikotarpiu rinkėjui patikrinti, ar jo užkoduotas balsas iš tiesų yra saugomas elektroninėje balsadėžėje;

Praktika rodo, kad tokiomis patikrinimo galimybėmis naudojasi labai mažas skaičius žmonių. Nenaudojant patikrinimo yra didelė tikimybė, kad už rinkėją nubalsavo kompiuterinis virusas.

Įstatyme reikėtų numatyti ne tik patikrinimo galimybę, bet ir nurodyti, kad patikrinimas yra privalomas ir be jo balsas nebus įskaitytas.

12 straipsnis. Rinkėjo balso patikrinimo principai

[...]

3. suskaičiuota kaip balsuota: tai principas, kuris turi užtikrinti, kad stebėtojai ar nepriklausomi auditoriai galėtų patikrinti, ar rezultatai yra gauti iškodavus elektroninėje balsadėžėje buvusius užkoduotus balsus;
4. tinkamas rinkėjas: tai principas, kuris turi užtikrinti, kad stebėtojai ar nepriklausomi auditoriai galėtų įsitikinti, kad visus skaičiuoti pateiktus rinkėjų balsus pateikė rinkimų teisę turintys asmenys.

Įstatyme nėra apibrėžta kas yra „stebėtojas“ ir kas juo gali būti. Labai svarbu numatyti, kad stebėtojų skaičius, tenkantis vienai balsavimo apylinkei, būtų ne mažesnis nei stebėtojų skaičius rinkimų apylinkėse.

Priešingai nei popierinio balsavimo atveju, balsavimo internetu stebėti tiesiogiai neįmanoma. Todėl būtina viešai skelbti biuletenių, balsadėžės formato ir naudojamų kriptografinių algoritmų specifikacijas. Viešos specifikacijos leis stebėtojams visapusiškai tyrinėti biuletenius ir balsadėžę. Tai yra vienintelis įmanomas būdas stebėtojams įsitikinti ar balsadėžė nebuvo pažeista.

Stebėtojų darbas netenka prasmės, jei jiems bus suteikta vienintelė galimybė stebėti naudojantis vieno tiekėjo sukurta programine įranga, ir ypač, kai ji yra uždaro kodo.

13 straipsnis. Balsavimo paslapties užtikrinimas

[...]

2. Pasibaigus rinkimų dienai elektroninėje balsadėžėje esantys biuleteniai išrūšiuojami pagal rinkimų apygardas, atskiriami nuo rinkėjo asmens tapatybės duomenų, sumaišomi taip, kad nebūtų galima nustatyti ryšio tarp elektroninio rinkimų ar referendumo biuletenio ir jį pateikusio asmens tapatybės. Visi veiksmai elektroninėje balsadėžėje atliekami automatiniu būdu.

Šis paragrafas prieštarauja 3-ame straipsnyje aprašytam slaptumo užtikrinimo principui *„informacinėje sistemoje privalo būti užtikrinama, kad nė vienas asmuo, įskaitant ir informacinės sistemos valdytoją ir tvarkytoją, negalėtų susipažinti su rinkėjo balsu“*.

Šiame straipsnyje teigiama, kad asmens tapatybės duomenys bus susieti su biuleteniais ir vėliau automatiniu būdu biuleteniai bus atskirti. Tai suteikia galimybę Vyriausiajai rinkimų komisijai susipažinti su rinkėjų balsais.

14 straipsnis. Dvigubo balsavimo išvengimas

[...]

2. Jei internetu balsavęs rinkėjas rinkimų dieną atvyksta balsuoti į rinkimų apylinkę, apylinkės rinkimų komisija nedelsdama privalo apie tai pranešti informacinės sistemos tvarkytojui, kuris informacinėje sistemoje pažymi, kad rinkėjas atvyko balsuoti į rinkimų apylinkę, ir iš elektroninės balsadėžės pašalina rinkėjo internetu paduotą elektroninį rinkimų ar referendumo biuletenį. Esant techninėms galimybėms ir apylinkių rinkimų komisijai rinkėjų sąrašuose pažymėjus, kad rinkėjas atvyko balsuoti, rinkėjo internetu paduotas elektroninis rinkimų ar referendumo biuletenis iš elektroninės balsadėžės pašalinamas automatiniu būdu.

Norint užtikrinti balsavimo slaptumą ir patikimumą VRK negali turėti galimybės pašalinti biuletenius iš balsadėžės tuo labiau identifikuodama balsavusį asmenį. Balsą pašalinti gali tik pats rinkėjas, naudodamas tik jam žinomą kriptografinę paslaptį.

15 straipsnis. Balsavimo internetu auditas

[...]

3. Informacinės sistemos auditas turi apimti [...] internetu paduotų balsų [...] saugojimą ir sunaikinimą [...]

Pasibaigus balsavimui balsadėžė neturi būti sunaikinama. Sunaikinus balsadėžę nebelieka jokių įrodymų ar balsai buvo suskaičiuoti teisingai. Remiantis 12-ame straipsnyje pateiktais rinkėjo balso patikrinimo principais, kiekvienas rinkėjas turi turėti galimybę atsisiųsti visą balsadėžę ir įsitikinti, kaip nurodyta ar jo balsas buvo įskaitytas ir suskaičiuotas taip, kaip nurodyta 12-ame straipsnio pirmuose trijuose principuose.

Pilnai įsitikinti ar balsas buvo įskaitytas ir suskaičiuotas galima tik atsisiuntus visą balsadėžę, kaip įrodymą.

15 straipsnis. Balsavimo internetu auditas

[...]

6. Informacija apie informacinės sistemos struktūrą, veikimą, šios sistemos programinės įrangos kodą ir jo pakeitimus turi būti prieinama tik tiems asmenims, kurie pasirašė informacinės sistemos valdytojo nustatytos formos sutartį dėl informacijos konfidencialumo.

Tiek Estijos, tiek Norvegijos balsavimo internetu sistemos yra atviro kodo ir norint susipažinti, kaip veikia sistema, nėra taikomi jokie apribojimai. Uždaro kodo sistema ir konfidencialumo sutartis kelia nepasitikėjimą sistema.

Toks reikalavimas aiškiai parodo, kad net jei sistema yra nepatikima - tai gali likti paslaptyje.

16 straipsnis. Kiti pagrindiniai balsavimo internetu reikalavimai

[...]

4. Atpažinus rinkėją elektroninėje erdvėje, visa informacija apsikeičiama naudojantis saugiu duomenų apsikeitimo protokolu.

Įstatyme būtina nurodyti, kad duomenų apsikeitimo protokolas turi būti atviras. Tai suteikia galimybę skirtingiems tiekėjams pasiūlyti konkurencingą programinę įrangą, skirtą balsavimui internetu. Balsuojantieji galės rinktis vieną iš daugelio būdų balsuoti internetu.

Rinkėjai, turintys techninių žinių, galės patys susikurti priemonę balsavimui internetu.

Jei protokolas bus uždaras, balsavimas internetu bus įmanomas naudojantis tik vieno tiekėjo programine įranga, o tai mažina pasitikėjimą balsavimu internetu.

16 straipsnis. Kiti pagrindiniai balsavimo internetu reikalavimai

[...]

5. Elektroninis rinkimų ar referendumo biuletenis turi būti užkoduojamas rinkėjo kompiuteryje ar kitame rinkėjo įrenginyje. Interneto ryšio kanalais negali būti perduodama nekoduota informacija.

Būtina pabrėžti, kad duomenims koduoti rinkėjas turi naudoti savo kompiuteryje ar kitame įrenginyje generuotas asimetrinio šifravimo raktų poras. Kvalifikuotas parašas turi būti naudojant tik asmens identifikavimui, bet ne biuletenio kodavimui. Tokiu būdu bus užtikrinta, kad niekas, įskaitant sertifikatą išdavusią instituciją, negalės klastoti biuletenio.

18 straipsnis. Įstatymo įgyvendinimas

1. Lietuvos Respublikos Vyriausybė kartu su Vyriausiąja rinkimų komisija iki 2018 m. sausio 1 d., vadovaudamosi šio ir Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymų reikalavimais, įsteigia ir įteisina Balsavimo internetu informacinę sistemą.

Būtina pabrėžti, kad prieš pradedant sistemos įgyvendinimą, turi būti parengta sistemos techninė specifikacija, kuri turi būti pateikiama kaip įstatymo priedas. Techninės specifikacijos po patvirtinimo nebegalima keisti, kadangi kiekviena balsavimo internetu protokolo detalė yra labai svarbi saugumo prasme.

Prieš pradedant kurti sistemą būtina patvirtinti techninį balsavimo internetu protokolą (techninę specifikaciją) ir tik tuomet imtis jos įgyvendinimo.

Parengtą techninę specifikaciją turi įvertinti ir patikrinti saugumo ekspertai ir kriptografijos specialistai.