Vertimas iš anglų kalbos, originalą galite rasti adresu -
http://www.parliament.uk/documents/speaker/digital-democracy/Digi072IanBrown.pdf

Informacinės politikos tyrimų fondo

atsakymas **Jungtinės Karalystės Parlamento pirmininko**
Skaitmeninės demokratijos komisijai

Informacinės politikos tyrimų fondas yra nepriklausoma organizacija, nagrinėjanti informacinių technologijų ir visuomenės sąveiką. Fondo tikslas – nustatyti svarų socialinį poveikį turinčią techninę plėtrą, siūlyti ir atlikti viešosios politikos galimybių tyrimus, skatinti visuomenės supratimą, bendradarbiavimą tarp technologiškai įgyvendinančių ir politiką formuojančių žmonių Jungtinėje Karalystėje (JK) ir Europoje.

Informacinės politikos tyrimų fondas teikia šias pastabas atsakant į Parlamento pirmininko Skaitmeninės demokratijos komisijos iškeltus klausimus apie elektroninį balsavimą:

1. Leidimas balsuoti nuotoliniu būdu, naudojant asmeninį kompiuterį ar telefoną, atrodytų patrauklus būdas norint supaprastinti rinkimų procedūrą ir padidinti dalyvaujančių rinkėjų skaičių – kiekvienas šiuos tikslus palaikytų.

2. Jau keletą metų „Rinkimų reformų bendrija“ ir kitos organizacijos reguliariai naudojo elektroninį balsavimą tokiuose žemesnės svarbos rinkimuose, kaip renkant vadovybę profesinėse organizacijose.

3. Kad ir kaip bebūtų, visgi ši technologija vis dar turi reikšmingų problemų, susijusių su saugumu, balsavimo slaptumu, atsparumu išorinei įtakai, kontroliavimu, aiškumu – kas užkerta kelią elektroninį balsavimą naudoti aukštesnės svarbos rinkimuose, kuriuose pajėgūs ir aprūpinti dalyviai (politinės partijos, suinteresuotos grupės ar netgi užsienio vyriausybės) gali būti suinteresuoti manipuliuoti tokia sistema.

4. Techninės saugumo spragos atsiranda iš nepakankamai apsaugotų esamų vartotojų sistemų bei interneto infrastruktūros. Dažniausiai asmeniniai kompiuteriai ir išmanieji telefonai yra nesunkiai prieinami kenkėjiškai programinei įrangai (bet kuriuo metu apie 5 proc. kompiuterių yra užkrėsti). Įsilaužus į įrenginius jų naudotojai nebegali kontroliuoti, ką šie įrenginiai daro jų vardu. Juodojoje rinkoje prieigomis prie tokių pažeistų įrenginių prekiauja brukalų prekiautojai, nusikaltėlių gaujos ir kiti pažeidėjai (įskaitant ir valstybinį lygmenį), kurie paprastai gali pasinaudoti tokiais duomenimis norėdami pakeisti JK rinkimų (ar referendumo) rezultatus, įgaudami vos keleto procentų persvarą pagrindinėse ribinėse rinkimų apygardose.

5. Saugumo klausimą dar labiau apsunkina griežti reikalavimai privatumo užtikrinimui. Internetinės bankininkystės, elektroninės prekybos ir kitų internetu paremtų sistemų apsauga remiasi informacijos apie atliktas transakcijas prieinamumu trečiosioms šalims, kurios gali sužinoti šią informaciją ir ją pakeisti. Tokiu atveju banko klientas, kurio kompiuteris yra užkėstas „*Dzeuso*“ kenkėjiška programa, kuri savavališkai atlieka pavedimus, gali būti apsaugotas, kai bankas pastebi ir užblokuoja tokius mėginimus atlikti neteisėtus pavedimus. Kitu atveju bankas grąžina tokias lėšas išsiaiškinus sukčiavimo atvejį. Su balsavimu yra nepalyginamai sunkiau, kadangi ypač sunku suderinti privatumą ir kontrolę.

6. Tai susiję su atsparumu išorinei įtakai. Galimybės balsuojančiam atskleisti savo balsavimo pasirinkimą turi būti ribotos, kitu atveju jis gali būti papirkinėjamas ar gąsdinamas. Šiuo metu mes tą pasiekiame duodant rinkėjams biuletenį balsavimo apylinkėje, kurioje yra balsadėžės, ir tarp rinkimų stebėtojų nėra politikos dalyvių.

(Bet netgi ši sistema nėra tobula; balsuojant tokiu būdu organizatoriai duoda rinkėjui užpildytą biuletenį prieš jam einant į balsavimo kabiną ir jis tikisi į balsadėžę įdėti būtent šį biuletenį, o pateikęs tuščią biuletenį - reikalauti savo kyšio).

7. Perėjimas prie internetinio balsavimo, kai rinkėjo kodas atsiunčiamas elektroniniu paštu ir tuomet jis naudojamas rinkimų puslapyje (taip yra daroma šiandieniniuose žemesnės svarbos internetiniuose rinkimuose), paliks atviras galimybes kyšininkavimui, bauginimui ir išorinės įtakos darymui. Rinkėjais manipuliuoti galėtų ne tik nesąžiningi politikos veikėjai (kaip „karuselės“ atveju), bet ir šeimos nariai bei kiti suinteresuoti asmenys. Yra buvę daug pasiūlymų, kaip internetinį balsavimą padaryti atsparesnį išorinei įtakai, pvz. suteikiama galimybė balsuoti keletą kartų, bet skaičiuojamas tik paskutinis internetu atiduotas balsas. Visgi nei vienas iš teiktų pasiūlymų nėra idealus.

8. Atsparumas išorės įtakai taip pat yra sunkiai sukontroliuojamas, kadangi netikėtas rezultatas (ar neženkli persvara) gali sukelti teisinį ginčą ir rezultatai turėtų būti perskaičiuoti. Mėginimai modeliuoti rinkimus, kurie būtų tiek atsparūs išorinei įtakai, tiek kontroliuojami, neišvengiamai veda prie sudėtingų schemų, į kurias įeina suklastoti biuleteniai ar programinė įranga paremta sudėtinga kriptografine matematika. Pabrėžiame - nei vienas iš pateiktų būdų nėra idealus ir tik keletas iš jų yra suprantami eiliniams rinkėjams (ar politikams), kurie neturi išsilavinimo saugumo inžinerijos srityje.

9. Rinkimų sistema turi būti suvokiama, siekiant įgyti ir išlaikyti visuomenės pasitikėjimą. Paprastai pasakymas „Vyriausybės Komunikacijos štabo matematikai nustatė, kad ši schema yra patikima, bet saugumo sumetimais mes negalime atskleisti jums detalių, tiesiog pasitikėkite mumis“ deja neveikia. Sąmokslo teorijos atstovai galės įrodinėti savo ir mažumos iškels savo abejones, siekdami diskredituoti rinkimus ir netgi suabejoti pačia demokratija.

10. Dabartinė sistema, kai biuleteniai skaičiuojami miestų savivaldybėse tiesiog ant stalų stebint rinkimų stebėtojams (parinktiems iš konkuruojančių kandidatų ir politinių partijų), yra geras saugumo, privatumo, atsparumo išorės įtakai, kontrolės ir paprastumo derinys. Nei viena internetinio balsavimo sistema nėra arti to.

11. Pastarąjį dešimtmetį šiuos klausimus savo ataskaitose nagrinėjo ekspertai. Mes iš jų rekomenduojame dvi, kurių išvados yra galiojančios:
    a. David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). Report to the Department of Defense (DoD) Federal Voting Assistance Program (FVAP), January 20, 2004.[1]
    b. Jason Kitcat. Electronic Voting: A challenge to democracy? Open Rights Group briefing paper, January 2007.[2]

12. Šios ataskaitos taip pat sprendžia keletą kitų Jūsų keltų klausimų – pavyzdžiui, kad yra mažai įrodymų, jog iki šiol internetinis balsavimas turėjo svarų indėlį rinkimuose. Atvirkščiai, rinkėjai jaučiasi drąsiau manydami, kad jie turi pasirinkimą ir galimybę kažką pakeisti – puikus to pavyzdys galėtų būti ką tik įvykęs referendumas Škotijoje.

[1] http://www.cs.berkeley.edu/~daw/papers/servereport.pdf
[2] https://www.openrightsgroup.org/wp-content/uploads/org-evoting-briefing-pack-final.pdf

Keliami klausimai apie rinkimuose nedalyvaujančius rinkėjus, kurie neturi galimybės pasinaudoti kompiuteriu ar išmaniuoju telefonu, ar kitu tinkamu ryšio įrenginiu.

Nacionalinis statistikos biuras ištyrė, kad 2014 metais 13 proc. suaugusiųjų JK yra niekada nesinaudoję internetu[3], tuo tarpu Ofcom Ryšių tyrimo ataskaita[4] (9 psl.) teigia, kad 8 proc. JK būstų esantis plačiajuostis internetinis ryšys yra lėtesnis nei 2Mb/s. Verta turėti omenyje, kad Glazge, kuris atrodo nusivylęs Škotijos referendumu, yra mažiausias plačiajuosčio interneto naudojamas iš visų Europos miestų.

13. Po neseniai atlikto Estijos elektroninio balsavimo tyrimo, kurį atliko Europos ir Amerikos saugumo tyrėjai ir rinkimų auditoriai, padarytos tokios išvados:

> *Yra įvairių būdų, kaip valstybinio lygmens nusikaltėliai, patyrę interneto nusikaltėliai ar nesąžiningi asmenys, turintys vidinės informacijos, galėtų atakuoti Estijos internetinio balsavimo sistemą. Toks nusikaltėlis galėtų nesukeldamas įtarimų pakeisti balsus, sužlugdyti rinkimus, sukelti abejones dėl rezultatų teisingumo. Šias rizikas yra sudėtinga eliminuoti, kadangi jos kyla iš pagrindinių architektūrinių pasirinkčių ir pagrindinių saugumo bei skaidrumo apribojimų, kurie gali būti įvesti atliekant kontrolę. Dėl šių priežasčių mes rekomenduojame Estijai nutraukti internetinio balsavimo sistemos naudojimą.* [5]

14. Mūsų nuomone internetinio balsavimo technologijos pritaikymas sukeltų ypač rimtų iššūkių JK rinkimų sąžiningumui ir kiltų rizika svarbiuose gyventojų sluoksniuose prarasti žmonių pasitikėjimą demokratija, ko priešingai siekia Komisija – jį stiprinti.

15. Galiausiai, žmonės, besipriešinantys šiuolaikinių technologijų naudojimui nusistovėjusiose veiklose, kartais yra vadinami senamadiškais ir savo neišmanymu užkerta kelią pokyčiams. Elektroninio balsavimo atveju, mes tikime, kad kuo labiau žmonės yra įsigilinę į technologiją, tuo labiau jie suvokia didžiules grėsmes, kylančias demokratiniuose procesuose. Nežinia verčia žmonės manyti, kad elektroninis balsavimas yra nerizikingas ir patrauklus. Ir tokie techniniai ekspertai, kaip mes (ir mūsų kolegos, kruopščiai patikrinę visą informaciją, kurią mes čia cituojame), įspėjame dėl elektroninio balsavimo artimiausioje ateityje.

Ian Brown
Informacijos Saugumo ir Privatumo Profesorius
Oksfordo Interneto Institutas
Oksfordo Universitetas

Anne-Marie Oostveen
Mokslinė bendradarbė
Oksfordo Interneto Institutas
Oksfordo Universitetas

Ross Anderson FRS FREng
Saugumo Inžinerijos Profesorius
Kompiuterių laboratorija
Kembridžo Universitetas

2014 m. rugsėjo 27 d.

[3] http://www.ons.gov.uk/ons/rel/rdit2/internet-access---households-and-individuals/2014/stb-ia-2014.html#tab-Computer-and-Internet-Use
[4] http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr14/2014_UK_CMR.pdf
[5] D Springall, T Finkenauer, Z Durumeric, J Kitcat, H Hursti, M MacAlpine, and JA Halderman. Security Analysis of the Estonian Internet Voting System. *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS'14)*, November 2014, at https://estoniaevoting.org/findings/paper/