31.01.2026

PUUDUSE AVALDUS

Lgp RVT!

Olete oma veebilehel 27.01 avaldanud seisukoha, et "e-hääletamine on turvaline ning põhjalikult auditeeritud". Avaldus annab märku mitmetest puudustest, mis on käsitletavad puudustena valimiste korralduses RKVS §68 tähenduses.

1. TTÜ doktorant Tarvo Treier tuvastas oma teadustöös 37 eri viisi, kuidas siseründaja, sh RVT võiks valimistel manipuleerida e-häältega. Doktorant valis neist katsetamiseks välja 17 praktilisemat, mida eksperimentaalselt katsetas ka 2024. aasta ja 2025. aasta valimistel reaalselt kasutusel olnud töötlemisrakenduste ja auditeerimisrakendusega. Neist 17-st praktilisest ründest 12 osutusid auditirakendusele tuvastamatuks, sj jättis doktorant läbi katsetamata ülejäänud 20 rünnet, mille kohta olemasoleva teadmise põhjal eeldas, et neid ei saaks auditirakendus kindlasti tuvastada. RVT aga ei nõustu doktorandi uurimistöö tulemustega ja väidab, et nende rünnete abil polnud võimalik tühistatud, korduvate vm e-häälte äravahetamisega manipuleerida tulemusi auditirakendusele märkamatult. Kui doktorandi tuvastatud rünnete nimekiri ei võimalda osutatud *circa* 8000 e-häälega manipuleerida, siis pole põhjust veatult töötavat auditirakendust täiendada ja RVT plaanib kulutada ressurssi ebavajalikele töödele. Minu kui valija ja kodaniku maksuraha kulutamine e-hääletamise auditeerimise süsteemi täiendustele, mida tegelikult pole vaja, on vastutustundetu ning käsitlen seda puudusena valimiste korralduses.

2. RVT väidab, et elektroonilise hääletuse süsteem on ehitatud selliselt, et audiitori läbiviidavad manuaalsed või automatiseeritud kontrollid ei mõjuta mitte kuidagi seda, kas e-hääli võidakse e-hääletuse mõnes etapis seadusvastaselt lisada, kustutada või muuta või kas selline seadusvastane tegevus avastatakse. Kui RVT seisukoht vastab tõele, siis ei täida audiitor praeguses e-hääletuse korralduses oma RKVS §48^8 lg11 vastavat ülesannet tagada protsesside sisendi ja väljundi ehk antud hääle ja kindlaks tehtud tulemuse omavaheline vastavus, terviklus ja autentsus. RVT väidetel võib olla tõepõhi all, sest doktorant Treieri uurimistöös kirjel-

datud 12+20 = 32 rünnet ei püüdnud audiitor tõepoolest 2025. aasta KOV valimiste auditeerimisel tuvastada, sest sellisest tegevusest ei leia jälgi ei audiitori lõpparuandest ega 20.10 läbi viidud toimingute videost. Kui audiitor RVT-le teadaolevalt ei täida endale seadusega pandud ülesannet, siis on see puudus valimiste korralduses, mis võis olla RVT-le teada juba 18.02.2025, mil Tarvo Treier informeeris RVTd osutatud 37 ründest, aga oli tõendatult teada hiljemalt 12.06.2025, mil doktorant edastas RVT-le tegelike e-häälte jm artefaktide kogumi, mis võimaldavad ründeid 2024. aasta ja 2025. aasta valimiste e-häältusel kasutusel olnud töötlemis- ja auditirakenduse puhul praktiliselt demonstreerida. Seejuures väljendab Tarvo Treier teadusartiklis ootust, et rünnetega arvestatakse 2025. aasta KOV valimiste ettevalmistamisel. Kui audiitor neid ründeid ei tuvasta ega saagi tuvastada, siis on see puudus valimiste korralduses, millest peaks RVT viivitamatult informeerima VVK-d, et see saaks võtta kasutusele talle seadusega ette nähtud meetmeid ja piirata eleketroonilise hääletuse kasutamist, kuni selle turvalisus ja valimisseaduse nõuetele vastavus on tõendatult tagatud. Kuna VVK koosolekute protokollidest ei nähtu, et RVT oleks VVK-d sellest puudusest valimiste korralduses informeerinud, siis on see informeerimata jätmine omakorda puudus valimiste korralduses ning see tuleks eeldatavasti ületada.

3. Doktorant Tarvo Treier oma uurimistöös püüdis hinnata elektroonilise hääletuse dokumentatsioonile ja auditiraportitele tuginedes, kas audiitor võis läbi viia kontrolle, mis võiks demonstreeritud 37 ründe läbiminemist välistada. Doktorant ei leidnud sellele avalikest materjalidest, sh tegelike valimiste auditiraportitest kinnitust, et audiitor oleks praktikas võtnud ette selliseid samme, mis siseründaja poolt läbiviidavad praktilised ründed oleks saanud tegelikel valimistel reaalselt välistada. Doktorandi poolt avalike allikate põhjal antud hinnangutest lähtuvalt ei ole maandatud siserünnete praktilised riskid, mida ta demonstreeris eksperimentaalselt tegelikel valimistel kasutusel olnud töötlemisrakenduse ja auditirakenduse identsete koopiate abil, kasutades eksperimendi läbiviimiseks enda loodud reaalsete elektrooniliste häälte kogumit. Kristjan Düüna ja Tarvo Treieri varasemad tööd, aga ka Treieri 2025. aasta töö näitlikustab praktiliselt ODIHRi 2023. aasta vaatlusraporti lk 7 ja alamärkuses 15 osutatud võimalust, et piisavaid vahendeid omav siseringi kuuluv isik “võib,

kui ta suudab seda teha märkamatult, kontrollida, millised hääled eemaldatakse, ja seega osaliselt mõjutada tulemusi". Kui ODIHRi tähelepanek oli esitatud allmärkuse vormis ja näitlikustas elektroonilise hääletuse süsteemi läbiva kontrolli (E2E-V) puudumist, siis Treieri uurimistöö näitlikustas seda praktiliselt, viies läbi eksperimendi tegeliku valimistarkvara ja tegelike häältega tegelikus arvutisüsteemis. Seega polnud Treieri töö mitte teoreetiline, vaid eksperimentaalne ja praktiline, mida ta demonstreeris ka Riigikogu korruptsioonivastase erikomisjoni nn vabal arutelul. Avalike allikate, sh auditiraportite põhjal antud hinnangutest lähtuvalt ei ole kasutusel meetmeid, mis sellised riskid maandaks ja kui RVT valduses on salajasi allikaid, mis selliste riskide maandamist tõendada võiks, siis on tegu puudusega valimiste korralduses ning sellised salajased materjalid tuleks viivitamatult avalikult kättesaadavaks teha, et demokraatlik üldsus, sh audiitorid ja valimisvaatlejad võiks hinnata, kas Treieri demonstreeritud praktilised siseründed, mille käigus RVT saab audiitorile märkamatult valimistulemusi võltsida, olid kuidagi maandatud 2025. aasta KOV valimistel (või saavad maandatud edaspidi, mille kohta puudub samuti RVT segaste sõnumite kontekstis mistahes arvestatav kindlus).

4. RVT väidab, et e-häälte manipuleerimiseks korduv- ja topelthäälte tühistamise käigus (mille võimalikkust RVT oma sama seisukohavõtu eelnevate lõikude väidetes kategooriliselt eitab) kasutatava pahavara olemasolu välistamise tarvis "kasutatakse häälte töötlemiseks turvalist ja võrguühenduseta arvutit, millesse on paigaldatud vastav tarkvara, mis taolised ründed tuvastab". Hääli töödeldakse selleks spetsiaalselt ette nähtud ja ette valmistatud arvutis, mille kirjeldused on leitavad elektroonilise hääletamise käsiraamatus. Arvuti on tegelikkuses olnud Ubuntu opsüsteemiga arvuti, millega on viidud läbi elektrooniliste häälte töötlemist ja krüptograafilist segamist, sj sama arvutit kasutas oma toimingute läbiviimiseks 2025. aasta KOV valimistel ka audiitor. Avalikus dokumentatsioonis ei ole kirjeldatud "vastavat tarkvara", mis oleks sellesse Ubuntu opsüsteemiga töötlemisarvutisse paigaldatud, mis võimaldaks välistada doktorant Treieri kirjeldatud ründeid korduv- ja topelthäälte tühistamise käigus. Kuna selline tarkvara on RVT väitel töötlemisarvutisse paigaldatud, aga selle tarkvara kohta ei leia midagi dokumentatsioonist ega ole see leitav ka lähtekoodist

varamutes aadressil https://github.com/valimised/ivxv/, siis on jäetud see tarkvara dokumenteerimata ja selle lähtekood avaldamata. Kuna lähtekood ja dokumentatsioon tuli avaldada enne KOV valimiste algust, siis on selle tarkvara avaldamata jätmine puudus valimiste korralduses, mis tuleks viivitamatult ületada, et valijad, vaatlejad ja demokraatlik avalikkus saaks selle tarkvaraga dokumentatsiooni ja lähtekoodi tasemel tutvuda, et omalt poolt veenduda selles, et RVT või mõni teadmata siseründaja ei manipulereinud e-hääli korduv- ja topelthäälte tühistamise käigus.

5. RVT väide auditeerimise põhjalikkusest ei ühti Teaduste Akadeemia küberturvalisuse komisjoni 2024. aasta riskianalüüsiga, mis toob vaatlemise ja auditeerimise puudujäägid välja kuuest tähelepanuväärsest riskist tervelt kahes, mis väidavad, et 1) mõned valimiste etapid võivad jääda auditeerimata/vaatlemata, kuigi see oleks võimalik ja 2) mõned e-hääletamise etapid võivad jääda auditeerimata/vaatlemata, sest tänane protokoll seda ei võimalda. Seejuures toob ODIHR oma 2025. aasta õigusraporti soovitus tähisega "I" ja seda täpsustava paragrahvi 65 raames välja, et "hoolimata rangest kontrollist ja riskide vähendamise meetmetest on alati olemas oht, et süsteemi osad ei pruugi korrektselt toimida", st "ei pruugi olla kohe selge, kas hääled on kadunud, neid on lisatud või muudetud puhtalt elektroonilise teekonna jooksul hääletusseadmetest digitaalse valimiskasti kaudu kuni veebis avaldatud tulemuseni". ODIHRi hinnangul võivad sellised muudatused olla "põhjustatud mitte ainult tahtlikust manipuleerimisest, vaid ka tundmatutest tarkvaravigadest, mis võivad tekkida uuenduste või kahjurvara kaudu". ODIHR annab kooskõlas maailma teadlaste suhtelise konsensusega teada, et "teadlaste pakutud lahendus on läbiv kontroll (E2E-V), mis võimaldab kontrollida, kas lõpptulemus vastab valijate tahtele, isegi kui osa süsteemist ei tööta nõuetekohaselt". Vale ei pruugi olla RVT väljendatud seisukoht, et suurema automatiseerimisega vähendatakse vaidlusi selle üle, kas audiitor on saanud e-häälte korrektses töötlemises piisavalt veenduda, kuid ODIHRi ja Teaduste Akadeemia seisukohaga pole kooskõlas väide, et "valimistel kasutatavate rakenduste avalike lähtekoodide ja Tarvo Treieri loodud testandmete põhjal saab iga piisavate IT-teadmistega inimene ka ise veenduda, et e-hääled loetakse kokku korrektselt". Nimelt ei taga lähtekoodi uurimine ja testandmete

sellest kompileeritud süsteemist läbi jooksutamine, et tegelikus arvutisüsteemis ei esine tulemusi moonutavaid tarkvaravigu või tahtlikku manipulatsiooni. Sama lõigu alguses osutatud "matemaatiline" kontroll ei anna midagi, kui see ei moodusta terviklikku krüptoprotokolli, mis tagaks süsteemi läbiva kontrollitavuse (E2E-V), mille puudumist on heitnud Eesti e-hääletusele ette ODIHR juba 2011. aasta valimiste raportist ja kuigi 2017. aastal kuulutati läbiv kontroll välja IVXV protokolli sisseviimisega, pole ka see andnud põhjust anda selle teostamisele positiivset hinnangut ODIHRil, aga ka teistel rahvusvahelistel asjatundjatel või nende ühingutel, kelle seisukohti osutati Riigikogu korruptsioonivastase komisjoni 9.06.2025 koosolekul, kus viibis ka RVT, ja selle protokollis nr 67. Kui RVT on seisukohal, et edaspidi ei pea enam usaldama RVTd ega audiitorit ja Treieri testandmed ja avalik lähtekood välistavad 27.01 avalduse teises lõigus negatiivse stsenaariumina osutatud võimaluse e-hääli märkamatult lisada, kustutada või muuta, siis see seisukoht on rahvusvaheliste raportite ja teadustööde suhtelise konsensuse alusel ekslik. Tõendatult eksliku seisukoha aluseks võtmine elektroonilise hääletuse süsteemi täienduste plaanimisel on käsitletav puudusena valimiste korralduses ning puudulik seisukoht tuleks viivitamatult korrigeerida, et tagada elektroonilise hääletuse turvaline ning töökindel läbiviimine demokraatlike valimiste põhimõtetest lähtuvalt nagu need on määratletud valimiseadustes ning põhiseaduse eri paragrahvides.

6. RVT väidab, et on teinud TTÜ teadlastega koostööd alates 2024. aastast, kuid Tarvo Treier Riigikogu korruptsioonivastase erikomisjoni vaba arutelu käigus väitis, et tema on edastanud RVT-le üksnes oma teadustöö tulemused ega oma RVT-ga lähemat koostööd, nt koostöölepingut, mis teda millekski kohustaks või asetaks talle vastutuse selle eest, kas või kuidas RVT Treieri uurimistööde tulemusi kasutab. Seejuures viidi Tarvo Treieri ja Kristjan Düüna soovitustest lähtuvalt sisse muudatused auditeerimise korraldusse ning võeti 2024. aasta valimistel kasutusele auditirakendus nimega `IntegrityTool`. Selle rakenduse realiseeris aga RVT vigaselt nii, et funktsiooni `getValidInvalidSums` sisendiks olnud ühildumatute andmetüüpide `set` ja `list` käsitsemine tööriista ridadel 264-289 andis tulemuseks auditirakenduse töö läbikukkumise 2025. aasta KOV valimiste auditeerimise raames. Sellise tüübiteisendusvea tõttu

andis auditirakendus tulemuseks teate `E-valimiskasti verifitseerimise logid on terviklikud: ei`. Kui Tarvo Treier ja Kristjan Düüna olid RVT koostööpatnerid, siis võiks eeldada, et neil oli selle tarkvaravea eest oma vastutus, sest nad ei kontrollinud piisavalt, kas nende soovitused viidi ellu korrektselt. Samamoodi oleks võinud kontrollida `IntegrityTool`-i korrektsust audiitor, kelle ülesanne see kehtiva regulatsiooni kohaselt on, kuid audiitor ei märgi seda tüübiteisendusviga ka oma 2025. aasta KOV valimiste auditeerimise lõpparuandes, mis tähendab, et see jäi märkamata nii RVT-l kui RVT väidetavatel koostööpartneritel TTÜ-st kui ka RVT palgatud audiitoril. Kui RVT osutatud Tarvo Treier tegelikult 2024. aasta Euroopa Parlamendi valimisteks lisanunud "automatiseeritud krüptogrammide kontrolli" korrektsuse eest ei vastutanud ega vastuta ka oma 2025. aasta soovituste tegeliku elluviimise eest, siis peaks RVT oma teavituses sellise vastutuse puudumise selgelt välja tooma, sest demokraatlikul avalikkusel, sh valijatel, vaatlejatel ja audiitoritel on oluline teada, kes vastutab valimistel kasutatava tarkvara kvaliteedi eest ning peab tagama, et selles puuduvad vead, st kellega täpselt, mis tingimustel tehakse koostööd, mis on väidetava koostöö laad ja kuidas jaotatud vastutus. Seejuures väärib veel kord märkimist, et Tarvo Treier väljendas oma 2025. aasta teadusartiklis ootust, et tema ettepanekutega arvestatakse 2025. aasta KOV valimiste ettevalmistamisel, kuid seda ei tehtud.

Soovin, et RVT annaks mulle iga puuduse avalduses väljatoodud punkti kohta eraldi teada selles punktis väljendatud puuduse läbivaatamise tulemustest ja võetud meetmetest.

Märt Põder