Riigi
valimisteenistus

Riigikogu korruptsioonivastane erikomisjon
Pr Anastassia Kovalenko-Kõlvart

Teie: 28.10.2026 nr 2-7/26-295/1
Meie: 06.11.2026 nr 12-10/26-30/2

Vastus pöördumisele elektroonilise hääletamise turvalisuse tagamise kohta

Täname Teid pöördumise eest.

Elektroonilise hääletamise turvalisus põhineb mitmel üksteist täiendaval tehnilisel ja korralduslikul meetmel, sealhulgas krüptograafilistel kontrollidel, toimingute dokumenteerimisel, sõltumatul auditeerimisel ja avalikul vaatlemisel. Riigi valimisteenistus teeb koostööd teadlaste ja küberturvalisuse ekspertidega, et hinnata uusi ründestsenaariume ning täiendada elektroonilise hääletamise süsteemi ja selle auditeerimise võimalusi.

Vastame Teie küsimustele järgmiselt.

1. Ründestsenaariumide edastamine audiitorile

Riigi valimisteenistus on varasemale samasisulisele teabenõudele vastates selgitanud, et Tarvo Treieri 18. veebruaril ja 12. juunil 2025 saadetud materjalid ning nendega seotud e-kirjad, päised, metaandmed ja lisad ei ole säilinud. Samuti ei ole riigi valimisteenistus pidanud nende materjalide edastamise kohta kirjavahetust Riigi Infosüsteemi Ameti, Vabariigi Valimiskomisjoni ega audiitoriga. Seetõttu ei ole võimalik vastavat kirjavahetust väljastada.

Riigi valimisteenistus tutvustas Tarvo Treieri 2025. aasta teadustöö tulemusi audiitoritele 11. septembril 2025 toimunud veebipõhisel infopäeval. Infopäeva ei protokollitud ega salvestatud, mistõttu puuduvad selle kohta väljastatavad dokumendid ja salvestised.

Tarvo Treieri teadustöö keskendus elektroonilise hääletamise auditirakenduse analüüsile ja selle automatiseeritud kontrollivõimaluste täiendamisele. Teadustöös ei tuvastatud elektroonilise hääletamise süsteemis turvaprobleemi, vaid kirjeldati võimalusi auditeerimise täiustamiseks.

2. Siserünnete kontrollimine 2025. aasta kohaliku omavalitsuse volikogu valimistel

2025. a kohaliku omavalitsuse volikogu valimistel kontrolliti elektrooniliste häälte töötlemise ja lugemise korrektsust mitme üksteist täiendava meetmega.

Elektroonilise hääletamise süsteem on üles ehitatud selliselt, et häälte töötlemise eri etappides on võimalik kontrollida andmete terviklust. Selleks kasutatakse muu hulgas aheldatud logisid, krüptograafilisi ja matemaatilisi kontrolle ning sõltumatut auditeerimist.

Lossi plats 1a,
15165, Tallinn
T. +372 631 6540
E. info@valimised.ee
valimised.ee

Elektrooniliste häälte töötlemiseks kasutatakse turvalist võrguühenduseta arvutit, mille tarkvara ja töökindlust kontrollib audiitor. Häälte töötlemise toimingud tehakse mitme isiku osalusel ja audiitori juuresolekul.

Audiitori tehtud krüptogrammide tervikluse kontroll läbiti edukalt. Kontrolli tulemusel tuvastati, et anonümiseeritud, jaoskonnas hääletamise tõttu tühistatud ning korduvhäälteks tunnistatud häälte krüptogrammid sisaldusid riigi valimisteenistusele üle antud e-valimiskastis ning kontrollitud andmestikus ei olnud krüptogramme lisatud, muudetud, asendatud ega kustutatud.[1]

20. oktoobril 2025 toimus Riigikogu hoones elektrooniliste häälte korduslugemine ja tervikluse kontroll. Korduslugemise käigus kontrolliti muu hulgas juhuvalimi alusel, kas tühistati üksnes jaoskonnas hääletanud valijate elektroonilised hääled.

Tehtud kontrollid on dokumenteeritud audiitori lõpparuandes, sealhulgas punktis 2.4 „Häälte korduslugemine ja tervikluse kontroll“.[2]

Riigi valimisteenistus selgitas 27. jaanuaril 2026 avaldatud uudises „E-hääletamine on turvaline ning põhjalikult auditeeritud“[3], et Tarvo Treieri teadustöö keskendus auditeerimisrakenduse võimalustele ega käsitlenud seda, kas kirjeldatud teoreetilised siseründed on tegelikult elluviidavad või milliste meetmetega on vastavad riskid juba maandatud.

Häälte töötlemisel võimalike manipulatsioonide ennetamiseks ja tuvastamiseks rakendatakse nii tehnilisi kui ka korralduslikke turvameetmeid. Auditeerimise täiendava automatiseerimise eesmärk on võimaldada audiitoril senisest rohkem kontrolle iseseisvalt korrata ning muuta kontrollide tulemused paremini jälgitavaks.

E-hääletamise audiitorilt nõutakse rahvusvaheliselt tunnustatud CISA (Certified Information Systems Auditor) sertifikaati. Sertifikaadi omanik peab järgima ISACA kutse-eetika koodeksit, mis kohustab tegutsema objektiivselt, järgima kutsealaseid standardeid ja esitama auditi tulemustes kõik olulised asjaolud. Audiitor vastutab oma kutsealases tegevuses kasutatud kontrollimeetodite ja auditi järelduste eest. Riigi valimisteenistus lähtub sõltumatu audiitori hinnangust ja auditi tulemustest.

Kõiki auditeerimise käigus tehtud toiminguid ei ole eraldi videosalvestisena avaldatud. 20. oktoobril 2025 tehtud tervikluse kontrollist eraldi avalikku videosalvestist ei ole. Kontrollide tulemused on kajastatud audiitori aruandes.

3. Siseründeriskide maandamine 2027. aasta Riigikogu valimisteks

Riigi valimisteenistus täiendab 2027. aasta Riigikogu valimisteks elektroonilise hääletamise auditeerimise tarkvaralahendust.

Riigi valimisteenistus selgitas 9. detsembril 2025 avaldatud uudises „E-hääletamise auditeerimine saab koostöös teadlastega taas täienduse“[4], et arenduse eesmärk on võimaldada audiitoril iseseisvalt ja automatiseeritult korrata elektrooniliste häälte töötlemise kontrolle, mida riigi valimisteenistus teeb häälte töötlemisel valimispäeva õhtul.

[1] Auditi punktid 2.4 ja 5. Kättesaadav arvutivõrgus: https://www.valimised.ee/sites/default/files/2025-12/L%C3%B5pparuanne%20KOV2025%20e-h%C3%A4%C3%A4letuse%20audit%2022.12%201.asice.
[2] Kättesaadav arvutivõrgus: https://www.valimised.ee/sites/default/files/2025-12/L%C3%B5pparuanne%20KOV2025%20e-h%C3%A4%C3%A4letuse%20audit%2022.12%201.asice.
[3] Kättesaadav arvutivõrgus: https://www.valimised.ee/et/e-haaletamine-turvaline-ning-pohjalikult-auditeeritud.
[4] Kättesaadav arvutivõrgus: https://www.valimised.ee/et/e-haaletamise-auditeerimine-saab-koostoos-teadlastega-taas-taienduse.

Need kontrollid hõlmavad muu hulgas e-valimiskasti andmete terviklust, korduvhäälte arvestamist ning jaoskonnas hääletanud valijate elektrooniliste häälte tühistamist.

Senise auditeerimise raames kontrollib audiitor, et riigi valimisteenistus teeb vajalikud kontrollid nõuetekohaselt. Andmeauditi käigus kontrollib audiitor oma tarkvaraga elektrooniliste häälte lugemise etappide sisend- ja väljundandmeid. Uue lahenduse abil saab audiitor lisaks iseseisvalt korrata riigi valimisteenistuse tehtavaid häälte töötlemise kontrolle.

Tarvo Treier on oma teadustöö raames koostanud testandmed koos veaolukordade kirjeldustega, mille abil saab kontrollida auditeerimisrakenduse võimet tuvastada andmetes kõrvalekaldeid. Need võimaldavad nii audiitoril kui ka teistel piisavate IT-teadmistega isikutel sõltumatult hinnata rakenduse toimimist.

Täiendatud tarkvaralahenduse lähtekood avaldatakse enne elektroonilise hääletamise algust, kavandatult hiljemalt 13. veebruaril 2027.

Lisaks tarkvaralistele kontrollidele rakendatakse elektrooniliste häälte töötlemisel korralduslikke turvameetmeid. Häälte töötlemise toimingud tehakse mitme isiku osalusel, järgides nelja silma põhimõtet, ning sõltumatu audiitori juuresolekul. Andmete terviklust kontrollitakse elektroonilise hääletamise eri etappides.

Enne 2027. aasta Riigikogu valimisi hindab riigi valimisteenistus elektroonilise hääletamisega seotud riskid uuesti üle, arvestades muu hulgas teadusuuringutes kirjeldatud ründestsenaariume, sõltumatute ekspertide tähelepanekuid, seniste auditite tulemusi ning süsteemi tehtud muudatusi. Riskide ümberhindamise käigus vaadatakse üle olemasolevate turvameetmete piisavus ja vajaduse korral kavandatakse täiendavad meetmed riskide maandamiseks.

Enne valimisi tehakse süsteemile vajalikud turva- ja koormustestid ja muud vajalikud kontrollid. Koormustestid on tehtud ning turvatestimine jätkub. Elektroonilise hääletamise turvalisust ja infoturbe korraldust hinnatakse ka Eesti infoturbestandardi (E-ITS) nõuete alusel.

Riigi valimisteenistuse riskianalüüs ja riskikäsitlusplaan sisaldavad teavet elektroonilise hääletamise süsteemi turvameetmete, võimalike nõrkuste ja riskide käsitlemise kohta. Nendele dokumentidele on kehtestatud juurdepääsupiirang AvTS § 35 lg 1 p 9 alusel.

4. Muude siserünnete avastamine ja riskijuhtimise korraldus

Elektroonilise hääletamise turvalisuse tagamisel ei lähtuta üksnes teadustöödes kirjeldatud konkreetsetest ründestsenaariumidest. Süsteemi turvalisust hinnatakse tervikuna, arvestades teadaolevaid ohte, võimalikke uusi ründeviise ja tehnoloogilisi arenguid. Elektroonilise hääletamise süsteemi dokumentatsioon ja lähtekood on avalikud, mis võimaldab sõltumatutel teadlastel süsteemi analüüsida ning esitada tähelepanekuid selle turvalisuse kohta.

Riigi valimisteenistus analüüsib teadlaste ja küberturvalisuse ekspertide esitatud tähelepanekuid ning hindab nende põhjal süsteemi täiendamise vajadust.

Näiteks analüüsisid Austraalia Rahvusülikooli teadlased Tingfeng Yu ja Thomas Haines Eesti elektroonilise hääletamise süsteemi ülesehitust, turvaomadusi ja võimalikke haavatavusi. Teadlased kirjeldasid kümmet teoreetilist riski, kuid ei tuvastanud süsteemis kriitilisi turvanõrkusi ega leidnud tõendeid selle kohta, et kirjeldatud ründeid oleks Eesti valimistel kasutatud.

Riigi valimisteenistus vaatas teadlaste esitatud leiud koos arenduspartneriga läbi ning hindas nende asjakohasust ja täiendavate meetmete vajadust. Osa kirjeldatud riskidest on maandatud varasemate arendustega, sealhulgas 2025. aastal kasutusele võetud uue krüptograafilise lahenduse ning auditeerimise täiendamise ja automatiseerimisega. Osa leidudest ei kohaldu Eestis kasutatavale süsteemile.

Kaks teadlaste kirjeldatud leidu (UV-V1 ja UV-V2) puudutavad häälte töötlemist ja lugemist ning teoreetilist võimalust tekitada selle käigus hulgaliselt kehtetuid hääli. Sellised kõrvalekalded tuvastab andmete tervikluse kontrolli käigus auditirakendus.

Teadlaste soovituse põhjal otsustas riigi valimisteenistus täiendada hääle kontrollrakendust registreerimisteenuse kontrolliga. Samuti analüüsitakse täiendavalt teisi asjakohaseid soovitusi.

See on näide sellest, kuidas sõltumatute teadlaste tähelepanekuid hinnatakse ning kasutatakse elektroonilise hääletamise süsteemi turvalisuse ja kontrollitavuse parandamisel.

Lisaks teadusuuringute analüüsimisele rakendatakse elektroonilise hääletamise turvalisuse tagamiseks mitmeid üksteist täiendavaid kontrollimehhanisme, sealhulgas krüptograafilisi tervikluskontrolle, toimingute dokumenteerimist, mitme isiku osalemise nõuet ning sõltumatut auditeerimist.

Riigi valimisteenistuse infoturbe korraldus hõlmab riskide tuvastamist, hindamist, käsitlemist ja seiret. Tuvastatud riskid ning nende maandamiseks kavandatud meetmed kajastatakse riskianalüüsis ja riskikäsitlusplaanis.

Enne 2027. aasta Riigikogu valimisi vaadatakse riskianalüüs ja riskikäsitlusplaan uuesti üle. Selle käigus hinnatakse ka seniste riskijuhtimise ja kontrollimeetmete piisavust ning vajadust täiendavate meetmete rakendamiseks. Infoturbe korralduse ja riskijuhtimise toimivust hinnatakse ka E-ITS-i auditeerimise raames.

5.–6. Elektroonilise hääle kehtivuse tõendamise riski käsitlemine

Riigi valimisteenistus on teadlik Tarvo Treieri teadustöös kirjeldatud võimalusest pahatahtlikul valijal kasutada elektroonilise hääletamisega seotud metaandmeid ja autentimistoimingute logisid selle tõendamiseks, milline elektrooniline hääl oli valija viimane ehk kehtiv hääl.

Kirjeldatud probleemi lahendamiseks on muudetud logiandmete kuvamist. Logides ei ole enam näha, et valija on suhelnud elektroonilise hääletamise serveriga. Seetõttu ei ole võimalik kirjeldatud logiandmete põhjal tõendada elektroonilise hääle andmise aega ega selle alusel tuvastada, milline elektrooniline hääl oli valija viimane kehtiv hääl.

Seega on teadustöös kirjeldatud logiandmete kasutamisega seotud probleem kõrvaldatud.

Riigi valimisteenistus hindab enne 2027. aasta Riigikogu valimisi elektroonilise hääletamisega seotud riskid uuesti üle, sealhulgas hääletamise salajasust ja valijale surve avaldamise võimalusi puudutavad riskid.

Juurdepääsupiiranguga dokumentide taotlemine

Pöördumises taotletakse muu hulgas dokumente, mis sisaldavad elektroonilise hääletamise süsteemi turvalisuse seisukohalt tundlikku teavet ning millele on kehtestatud juurdepääsupiirang AvTS § 35 lg 1 p 9 alusel.

AvTS § 38 lõike 3[1] kohaselt tuleb seaduses sätestatud juhul avalike ülesannete täitmiseks juurdepääsupiiranguga teabele juurdepääsu taotlemisel teatada teabevaldajale juurdepääsu õiguslik alus ja eesmärk.

Korruptsioonivastase seaduse § 9 lõike 2 kohaselt on Riigikogu korruptsioonivastasel erikomisjonil õigus oma ülesannete täitmiseks nõuda tutvumiseks andmeid ja dokumente.

Palume kinnitada, et juurdepääsupiiranguga dokumentide saamise taotlus on esitatud Riigikogu korruptsioonivastase erikomisjoni kui kollegiaalse organi nimel, ning edastada vastav komisjoni otsus või muu dokument, millest nähtub komisjoni tahe nimetatud andmeid ja dokumente taotleda. Samuti palume täpsustada taotletavatele dokumentidele juurdepääsu õiguslik alus ja eesmärk.

Saadud teabe alusel saame hinnata juurdepääsupiiranguga dokumentidega tutvumise võimaldamise tingimusi. Seejuures arvestame, et komisjonile dokumentidega tutvumise võimaldamine ei muuda juurdepääsupiiranguga teavet avalikuks.

Riigi valimisteenistus jätkab elektroonilise hääletamise süsteemi ja selle auditeerimise arendamist, lähtudes õigusaktidest, infoturbe nõuetest, sõltumatute ekspertide hinnangutest ning teadusuuringute tulemustest.

Lugupidamisega

(allkirjastatud digitaalselt)

Arne Koitmäe
Riigi valimisteenistuse juht