EESTI TEADUSTE AKADEEMIA

Teaduste akadeemia küberturvalisuse komisjoni koosoleku protokoll 18. detsembril 2024. aastal

Tartu Ülikooli raamatukogus ja Zoomi keskkonnas

Algus kell 10.30
Lõpp kell 15.00

Juhatas akadeemik Dan Bogdanov

Osalesid: akadeemik Anu Realo, Kati Ambo-Vaher, Arne Koitmäe, Alo Einla, Kristjan Krips, Ivo Kubjas, Priit Parmakson, Guido Pääsuke, Teet Raidma, Tanel Tammet, Ahto Truu, Jan Villemson, Priit Vinkel, külalisena Tõnis Lepik RIAst.

Protokollis: Ülle Sirk

1. **Mis tehtud, mis teoksil? Valimiste tehnoloogia ja õiguse alaste uudiste jagamine**

Arutelus osalesid kõik istungil osalejad

a) Kati Ambo-Vaher teatas, et VVK on arutanud nutiseadmel valimisi, kuid otsuseid pole tehtud.
b) Teet Raidma kinnitas Kati öeldut ning teatas, et VVK ootab ka TA küberturvalisuse komisjoni hinnanguid. Akadeemik Bogdanov selgitas, et sõltuvalt tänase istungi tulemitest on ehk võimalik panna kokku memo VVK-le. Teet Raidma palve on, et kui see dokument tuleb, siis enne 7. jaanuarit ja otse VVK-le.
c) Akadeemik Dan Bogdanovi soov on, et dokument oleks korrektses vormis, et sellest saaksid aru ka need, kes ei ole väga tugevalt kursis TA komisjoni tööga, et nad mõistaksid, mida komisjon teeb. Seega peaks kindlasti olema kaaskiri.
d) Ivo Kubjas mainib, et komisjon peaks hindama vajadust internetivalimiste läbiviimisel üle minna postkvant-krüptograafiale. Mitmed maailma riigid annavad välja strateegiadokumente, et lõpetada kvantarvutiga rünnatava krüptograafia kasutamine 2030. või 2035. aastaks. Akadeemik Dan Bogdanov palus, et Jan Villemson, kes on avaldanud mitmeid teadustöid postkvant-krüptograafia alal, koostaks vastava ohuanalüüsi komisjoni jaanuari istungiks.
e) Kristjan Krips märkis ära, et kvantarvutikindlus on ka üks turvaeeldus ning oleks viimane aeg valimiste tehnoloogiate turvaeeldused kirja panna.

Informatsioon võeti teadmiseks.

2. **Nutiseadmetega valimiste riskide ülevaade ja analüüs. See päevakorrapunkt sõltub teie tehtud kodutöödest**

Arutelus osalesid kõik istungil osalejad.

Töötati läbi kuus ette valmistud ohuanalüüsi, mille komisjoni liikmed on koostanud.

a) Ahto Truu - "Libavalijarakenduste ilmnemine Eestis ja maailmas rikub valimistulemuse terviklust või hääle salajasust". Ohtu analüüsiti, täiendati ja anti riskihinded.
b) Kristjan Krips - "Audiitor ei kontrolli valimisperioodi ajal rakendustepoodide kaudu levitatava valijarakenduse terviklust ja autentsust. Kontroll teostatakse enne valimiste algust.". Ohtu analüüsiti, täiendati ja anti riskihinded.
c) Anu Realo - "Nutiseadmelt internetivalimiste kasutuselevõtu kiirustamisega kahjustatakse valimiste usaldusväärsust tervikuna". Ohtu analüüsiti, täiendati ja anti riskihinded.
d) Alo Einla korraldab, et uuendataks "Valijarakenduse autentsus ei ole tõendatavalt auditeeritud". Ohtu analüüsiti, kuid ei hinnatud, sest eelmisest korrast kui seda ohtu hinnati, pole piisavalt palju muutunud. Kehtima jäi sama riskihinne.
e) Arne Koitmäe - "Ühes ringkonnas või ühel operatsioonisüsteemil läbi viidud nutiseadmega valimiste piloot rikub valimiste usaldusväärsust tervikuna." Ohtu analüüsiti, täiendati ja anti riskihinded.
f) Ivo Kubjas - "Nutiseadmete operatsioonisüsteemide paljusus tõstab koormust valimiste kasutajatoele". Ajapuudusel ohtu analüüsiti, kuid see jäi hindamata.

Informatsioon võeti teadmiseks.

3. **Arutelu selle üle, kas ja kuidas nutiseadmetel valimise riskianalüüsi tulemusi edasi anda**.

Otsustati, et TA küberturvalisuse komisjoni juht akadeemik Dan Bogdanov koostab VVK jaoks tänase istungi põhjal memo mustandi ning tutvustab seda komisjonile.

Järgmise koosoleku aeg

Järgmine koosolek toimub 7. jaanuaril 2025 Tartu Ülikooli raamatukogus, Tartus.