Tööde kirjeldus

Majandus- ja kommunikatsiooniministeerium (edaspidi MKM) viib läbi hanke, mille eesmärk on leida Eesti elanike küberturvalisuse teadlikkuse ja digitaalsete oskuste ülevaate uuringu läbiviija.

1. Taustainformatsioon

Küberriskide mõju võib olla erinev sõltuvalt vanusest, seoses iga grupi unikaalsete harjumuste ja tehnoloogiliste teadmistega. Lapsed ja noorukid kasutavad internetti aktiivselt mängudeks, sotsiaalmeediaplatvormide kasutamiseks ning õppetööks. Nad võivad olla haavatavad küberkiusamise, privaatsuse rikkumise ja pettuste ohvriks langemise osas, kuna neil võib puududa teadlikkus küberohtudest või nad ei pruugi tunda turvalise internetikasutuse põhitõdesid.

Laste ja noorukite poolt kasutatavad digitaalsed lahendused erinevad vanemate vanusegruppide poolt kasutatavatest lahendustest, kasutatavad sotsiaalmeediaplatvormid on generatsioonide lõikes erinevad ning sama kehtib ka küberturberiskide kohta, millega erinevad vanusegrupid kokku puutuvad.

Olenemata vanusest võivad noored, kes ei ole digitaalselt osavad või kellel puudub juurdepääs piisavale teadmusele, kergesti langeda ohvriks küberrünnakutele, nagu õngitsemine, identiteedivargus, pahavara või puutuda kokku teiste sarnaste küberohtudega.

Küberriskide maandamiseks on oluline roll haridusel ja teadlikkusel. Organisatsioonid, haridusasutused ja lapsevanemad peaksid pakkuma asjakohast koolitust ja juhiseid, tõstmaks teadlikkust ja oskusi küberohtude äratundmiseks ning nendega toimetulekuks laste ja noorte seas.

Senised küberkäitumise-alased uuringud on suuresti keskendunud eelkõige laiema elanikkonna küberkäitumisele ja küberhügieenile, uuematest uuringutest on II ja III kooliastme küberkäitumist käsitlenud TÜ eetikakeskuse RAYUELA (H2020 projekt „Noorte harimine ja jõustamine läbi mängimise internetis ohutult toimetamiseks“) projekt, mille raames läbi viidud fookusgrupi intervjuud II-III kooliastme Eesti õpilaste seas annavad ülevaate kokkupuudetest eri küberohtudega ja küberkuritegudega, niisamuti erinevustest eri rahvusgruppide seas (vt: RAYUELA - A fun way to fight cybercrime (rayuela-h2020.eu)). Projekti laiem eesmärk oli luua ülevaade noorte kokkupuudetest erinevate küberkuritegudega ning selle baasil luua mängulised tegevused, mille abil vastavas sihtrühmas ennetustööd teha. Digi- ja küberpädevus (edaspidi DKP) kompetentside kohta II ja III kooliastme noorte seas annavad ülevaate ka Kaitseministeeriumi poolt ellu kutsutud ja TalTechi küberkriminalistika ja küberjulgeoleku keskuse poolt läbiviidavad KüberPähkli uuringud ja test-võistlused, mille laiem fookus on testida õpilaste küberturbe-alaseid teadmisi, andes uuringuanalüüsi baasil soovitusi koolidele, lapsevanematele, riigile ja kohalikele omavalitsustele küberriskide maandamiseks vastava sihtrühma seas. Ülevaate Eestis läbi viidud küberkäitumise uuringutest annab ka Sisekaitseakadeemia sisejulgeoleku instituudi (2023) raport

“Eesti elanikkonna teadlikkus küberturvalisusest: ülevaade uuringutest ja võimalikest edasistest suundadest”.

Põhikooli riiklik õppekava (PRÕK 2011, § 4 lg 8) näeb ühe õppeeesmärgina ette digipädevuste arendamist. See eesmärk hõlmab endast põhikooli noorte seas infootsingute ja digitaalse sisuloome oskuste ja pädevuste arendamist, uute tehnoloogiatega toimetulekut ning teadlikkuse arendamist erinevate digikeskkondade ohtude märkamisel ja neile reageerimisel. DKP arendamine ja tehnoloogia/arvutiõpetuse sisuline pool ja fookus on koolide endi otsustada, seetõttu on vastavate pädevuste arendamise rõhk kooliti erinev. Lisaks PRÕKile sätestab tehnoloogiaõpetuse lisa (VV 28. jaanuari 2010. a määruse nr 14 „Põhikooli riiklik õppekava” lisa 7) ka alateema „Tehnoloogia ja innovatsioon“ digipädevuste arendamise, mida seostatakse eeskätt arvuti kasutamise võimaluste ja digikeskkonna kasutamisega, ent digipädevuste ja digitaalsete tehnoloogiate ja platvormide kasutamise oskuste arendamise puhul pole PRÕKis ega selle lisades eraldi esile toodud küberturvalisusega seotud õpiväljundeid- ja eesmärke. Sellest tulenevalt esineb koolide vaates DKP arendamisel olulisi erinevusi, kuna arvuti/informaatikaõpetus on põhikooliastmes valikuline. Arvuti/informaatikaõpetuse varieeruvust nenditakse ka Startup Estonia poolt tellitud ja Rakendusliku Antropoloogia Keskuse ja Eesti Uuringukeskuse poolt läbi viidud uuringus “Tuleviku tegija teekond: kas homsed oskused tulevad koolist, huviringist või YouTube’ist?” (2023), mille laiem fookus oli kaardistada tegureid, mis suurendavad noorte seas huvi MATIK (matemaatika, teaduse, tehnoloogia, inseneeria ja kunstid) valdkondade vastu.

2. Hanke eesmärk

Hanke eesmärk on leida koostööpartner, kes koostab küberturvalisuse teadlikkuse ja digitaalsete oskuste ülevaate II ja III kooliastme noorte seas. Lisaks annab hanke raames koostatud analüüs soovitusi erinevate õppematerjalide koostamiseks, loomaks turvalisemat digitaalkeskkonda, tõstes seeläbi teadlikkust ja oskusi vastava sihtrühma seas ning andes sisendit asjakohasele poliitikale ja sekkumisstrateegiatele, mis vastavad II ja III kooliastme noorte unikaalsetele vajadustele. Samuti on hanke eesmärgiks pakkuda väärtuslikku panust küberjulgeoleku valdkonna arengusse, aidates kujundada turvalisemat digitaalset tulevikku. Majandus- ja Kommunikatsiooniministeeriumi koostatud küberturvalisuse strateegias (“Läbivalt IT-vaatlik Eesti”) aastateks 2024-2030 on samuti esile toodud küberturvalisuse valdkonna järelkasvu dimensioon, mistõttu on hanke raames koostatud analüüsi üheks oluliseks elemendiks järelkasvu soodustamine. Seega on analüüsi üheks mõõtmeks uurida tegureid, mis soodustaksid II ja III kooliastme noorte seas DKP arendamist laiemalt ning suurendaksid huvi küberturvalisuse valdkonna vastu. Küberspetsialistide järelkasvu soodustamine on omakorda kriitiline, tagamaks küberkogukonna ja DKP teadmuse jätkusuutlikkus Eestis.

Seega tellitakse hankega tervikteenus, mille hulka kuulub:

- küberturvalisuse teadlikkuse ülevaate II ja III kooliastme õpilaste seas;

- küberturvalisuse õppematerjalide projekti sisendi loomine (vt täpsemalt p. 3.1.).

3. Hanke tulemusena sõlmitud lepingu täitmise tulemus

Käesoleva hanke tulemusena peab:

- valmima küberturvalisuse teadlikkuse teaduspõhine uuring, mis annab ülevaate küberturvalisuse teadlikkuse hetkeolukorrast, suundumustest ning mõjuteguritest II ja III kooliastme õpilaste seas. Tervikdokumendis peavad olema esile toodud riskide maandamiseks konkreetsed juhised ja soovitused küberteadlikkuse tõstmiseks ja soovitusi efektiivseima õpiväljundi saavutamiseks.

3.1. Küberturvalisuse teadlikkuse analüüs

3.1.1. Üldine sisu ja nõuded

Paljudel inimestel puuduvad piisavad teadmised küberohtudest ja nende ennetamisest. Sihipärane analüüs võimaldab kohandada haridus- ja teavitusprogramme, mis on suunatud konkreetsete vanuserühmade vajadustele, et parandada nende küberturvalisuse-alast teadlikkust ja oskusi.

Erinevad vanuserühmad võivad olla küberriskidele erinevalt vastuvõtlikud, kuid praegused turvalahendused ei pruugi neid eripärasid arvestada. Käesoleva hanke raames koostatud analüüs peab aitama tuvastada II ja III kooliastme noorte spetsiifilised vajadused ja eripärad, töötamaks välja asjakohased koolitusmaterjalid ning loomaks ülevaade vastava sihtrühma digi- ja küberpädevustest (DKP).

Ühiskonnarühmade ebapiisav ettevalmistus ja reageerimisvõime küberrünnakutele võib põhjustada ulatuslikku kahju nii individuaalsel kui ka organisatsioonilisel tasandil. Analüüs peab toetama üldist vastupanuvõimet ja iga noore valmisolekut tuvastamaks küberrünnakuid. Sageli annavad noored enda vanematele ja vanavanematele digioskuseid edasi, arendades seeläbi vanemate digi-ja küberpädevusi, ent ka vanemad on sageli digioskuste arendamisel lastele eeskujuks. Uuring peaks andma ka lapsevanematele soovitusi DKP ja oskuste arendamiseks laste seas, tõstmaks seeläbi ka laiemat huvi küberturvalisuse valdkonna vastu. Uuringu eesmärk on välja selgitada küberturvalisuse teadlikkuse ja ohuhinnangute tasemed II ja III kooliastme noorte seas, sealhulgas toob analüüs esile tegurid, mis kujundavad noorte ohuhinnanguid ja teadlikkust ning tegurid, mis soodustavad DKP arendamist. Analüüsi keskmes on II ja III kooliastme noorte digi- ja küberpädevused, valim jaotub vastavalt kooliastmele, soole ning rahvuslikule kuuluvusele, hindamaks võimalikult laia sihtrühma seas erinevaid mõjutegureid ja tendentse.

Analüüs peab pakkuma tervikliku ülevaate küberturvalisuse teadlikkusest. Hankija näeb ette, et analüüs peab vastama eelmainitud eesmärkidele ja alljärgnevatele küsimustele:

- Kuidas noored tuvastavad ja reageerivad küberohtudele sotsiaalmeediaplatvormidel?;
- Kuidas mõjutada kõige paremini II ja III kooliastme noori, arendamaks digi- ja küberpädevusi ja laiemat huvi küberturvalisuse valdkonna vastu?
- Kas ja kuidas soodustab reaalainete õpe huvi DKP arendamisel?
- Millised on enimkasutatavad digitaalsed platvormid ja sotsiaalmeediaplatvormid II ja III kooliastme noorte seas?
- Kuidas erinevad isikliku teabe jagamise harjumused lastel ja lapsevanematel ning kuidas see mõjutab nende küberriski taset?; Millised on enimlevinud eksiarvamused ja ohtlikud praktikad II ja III kooliastme õpilaste seas teabe jagamisel internetis?
- Milline on koolide tase DKP õpetamisel ja arendamisel?
- Milline on koolide roll küberturvalisuse alase teadlikkuse tõstmisel II ja III kooliastme noorte seas?
- Milline on II ja III kooliastme noorte ja nende vanemate valmisolek ja võimekus tuvastada ja reageerida levinumatele küberrünnetele?;
- Kuidas arendada tõhusaid küberhügieeni harjumusi II ja III kooliastme noorte seas, kes kasvavad üles digitaalselt küllastunud keskkonnas?;
- Millised meetodid ja tehnoloogiad on kõige tõhusamad noorte pikaajaliseks kaasamiseks küberturvalisuse praktikatesse?;
- Kas ja kuidas erineb DKP omandamine poiste ja tüdrukute seas, II ja III kooliastmes? Kas ja kuidas esineb erinevusi erinevate keeleliste sihtrühmade DKP omandamise puhul?
- Milliseid DKP arendamise õppematerjale kasutatakse Eestis II ja III kooliastme noorte puhul? Milline on olemasoleva õppematerjali kvaliteet?;
- Millised on rahvusvahelised või Eestis läbi viidud sarnaste uuringute tulemused? Lisada vastava uuringu lühikokkuvõte ja viide uuringule.
- Millised tegurid ja sotsiaalsed keskkonnad mängivad enim rolli DKP omandamisel – on selleks näiteks kool, lähikondlased, sõbrad?
- Kas ja kuidas mängivad rolli mõjuisikud DKP arendamisel - mõjuisikuteks võivad olla lapsevanemad, õpetajad, suunamudijad, täiskasvanutest eeskujud.

Lisaks peab analüüs sisaldama ettepanekuid II ja III kooliastmele suunatud DKP arendavate õppematerjalide võimalustest, vastates alljärgnevatele küsimustele/punktidele:

- milliste teabekanalite kaudu on võimalik jõuda vastava vanuserühmani (II ja III kooliastme õpilased), milline on selleks parim võimalik teabekanal vastava kooliastme õpilaste seas?;
- millised on parimad võimalikud õppemeetodid ja eripärad vastavate kooliastmete noorte seas;
- millised on soovituslikud teabe edastuse formaadid (näiteks; video, audio, digitaalne- või trükitud tekst), arendamaks DKP vastava sihtrühma seas?

Eeltoodud loetelu on hankijapoolne visioon, milliseid komponente või aspekte tuleks küberturvalisuse teadlikkuse puhul uurida. Juhul, kui pakkuja soovib mõne aspekti/komponendi osas sisse viia täiendusi ja/või mõne hankija poolt välja toodud aspekti/komponendi uurimisest soovitakse loobuda, siis lepitakse selles kokku tööde teostamise käigus.

3.1.2. Uurimis- ja analüüsimeetodid

Hankija visioonis tuleks analüüsiprojekti läbiviijal uurimisküsimustele vastamiseks kasutada kombineeritud uurimis- ja analüüsimeetodeid, mis sisaldavad nt dokumentide analüüsi, kvalitatiivseid intervjuusid (süvaintervjuud või fookusgrupi intervjuud vms), kvantitatiivset andmeanalüüsi jm.

Täpne uurimis- ja analüüsimetoodika on pakkuja valida. Pakkujal tuleb meetodeid pakkumuses põhjendada ja selgitada. Pakutavast metoodikast peavad nähtuma kõikide uuritavate komponentide uurimis- ja analüüsimeetodid. Vajadusel täpsustatakse metoodikat tööde elluviimise käigus.

Muu

Projekt viiakse ellu Euroopa Liidu kaasrahastamisel ja tööde teostamisel tuleb sellele viidata. Täpsemad juhised ja vajaliku sümboolika edastab hankija tööde teostamisel. Analüüsi oodatav valmimisaeg on 4 (nelja) kuu jooksul alates lepingu sõlmimisest vastavalt tööde käigus kokku lepitule, kuid mitte hiljem kui 20. detsember 2024.

Töö käigus kogutavad andmed ja kaasnevad intellektuaalsest varast tulenevad õiguste

kasutusõigused (lihtlitsents koos all-litsentsiga) kuuluvad pärast töö üleandmist ministeeriumile. Ministeerium võib töö käigus kogutavaid andmeid ja intellektuaalsest varast tulenevate õiguste kasutusõigusi vabalt kolmandatele isikutele üle anda ilma uuringus osalejate nõusolekuta.