Kaisa Niilo

ADMINISTRATIIVTÖÖTAJATE DIGITURVALISUSE PÄDEVUSE HINDAMINE

LÕPUTÖÖ

Teenusmajanduse instituut
Teabehalduse ja infosüsteemide korraldamise õppekava
Juhendaja: Meelis Rebane, *MA*

Mõdriku 2022

Autori deklaratsioon ja lihtlitsents

Mina, Kaisa Niilo, tõendan, et lõputöö on minu kirjutatud. Töö koostamisel kasutatud teiste autorite, sh juhendaja teostele on viidatud õiguspäraselt.

Kõik isiklikud ja varalised autoriõigused käesoleva lõputöö osas kuuluvad autorile ainuisikuliselt ning need on kaitstud autoriõiguse seadusega.

Juhendaja Meelis Rebane, */allkirjastatud digitaalselt/*

Lõputöö on kaitsmisele lubatud teenusmajanduse instituudi direktori korraldusega nr 1-14/55 kuupäev 02.05.2022.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Kaisa Niilo

sünnikuupäev 22.07.1990,

annan Tallinna Tehnikakõrgkoolile (edaspidi kõrgkool) tasuta loa (lihtlitsentsi) enda loodud teose

ADMINISTRATIIVTÖÖTAJATE DIGITURVALISUSE PÄDEVUSE HINDAMINE

1. reprodutseerimiseks paberkandjal kõrgkooli raamatukogus avaldamise ja säilitamise eesmärgil;
2. elektroonseks avaldamiseks kõrgkooli repositooriumi kaudu;
3. kui lõputöö avaldamisele on instituudi direktori korraldusega kehtestatud tähtajaline piirang, lõputöö avaldada pärast piirangu lõppemist.

Olen teadlik, et nimetatud õigused jäävad alles ka autorile ja kinnitan, et:

1. lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid ega muid õigusi;
2. PDF-failina esitatud töö vastab täielikult kirjalikult esitatud tööle.

Tallinnas 03.05.2022 , */allkirjastatud digitaalselt/*

SISUKORD

SISSEJUHATUS

Eesti on tuntud oma riiklike digilahendustega, mis hõlbustavad elanike ja riigi vahelist suhtlust. Eesti on seejuures tõenäoliselt ainukene riik maailmas, kus 99% avalikke teenuseid on kättesaadavad internetis, olenemata ajast ja kohast (e-governance)**.** Selline ülesehitus paneb suure rõhu küberturvalisuse järgimisele ning digipädevuse arendamisele. Digipädevus on üks kaheksast elukestva õppe võtmepädevusest, millega 2014. aastal täiendati ka põhikooli ning gümnaasiumi riiklikke õppekavasid (Noorteamet). Uuenevat digitehnoloogiat õpetatakse õpilastele, kuid täiskasvanute järele aitamine selles valdkonnas on riiklikul tasemel lahendamata.

Euroopa Komisjoni Teadusuuringute Ühiskeskuse Tulevikutehnoloogiate Instituut töötas välja digipädevuste raamistiku (*Digital Competence Framework*, DigComp) mudeli 2013. aastal, mis on olnud juhiseks kodanike digipädevuste määratlemisel ja parandamisel Euroopa Liidus *(Awareness of the DigComp framework among the CEPIS community)*. DigComp digipädevuse mudel on enesehindamisevahend, milles on välja toodud viie valdkonna alapädevused ning need jagatud veel omakorda kolme pädevustasemesse (Ferrari, 2013).

Riigi Infosüsteemide Ameti (RIA) Küberturvalisuse aastaraamat võtab kokku 2021. aasta sagedasemad eraisikute ja ettevõtete nõrgast küberhügieenist tingitud eksimused ja küberturvalisuse intsidendid ning annab ülevaate järgneva perioodi eesseisvatest väljakutsetest. Möödunud 2021. aasta eristus eelmistest rohkete turvanõrkuste poolest. „Eesti küberruum on kaitstav, kui riik ja ühiskond tervikuna selle kaitsmises osalevad, kui selleks on ette valmistatud vastavad spetsialistid ning ühiskond teab virtuaalmaailma ohtusid ja oskab neid parimal viisil vältida ning probleemide korral reageerida“ (Kaitseministeerium). Ka tööjõu- ja oskuste vajaduse prognoosisüsteemi (OSKA) 2018. aastal läbiviidud uuringu „Tulevikuvaade tööjõu- ja oskuste vajadusele: personali- ja administratiivtöö ning ärinõustamine” väljavõte olulisematest tulemustest juhib tähelepanu, et kõigil uuringus olnud kutsealadel on kasvav vajadus üldiste teadmiste järgi küberturvalisusest. Ühtseid mõõdikuid piisava digipädevuse praktiliseks hindamiseks on aga vaid üksikutes valdkondades (nt kaitseministeeriumi valitsemisalas või õpetajate enesehindamisel). Intensiivselt info- ja kommunikatsioonitehnoloogia (IKT) vahenditega tööalaselt kokkupuutuvatel administratiivtöötajatel selline hindamisvahend puudub.

Eelnevast tulenevalt püstitab autor uurimisprobleemi: puudub administratiivtöötajatele kohandatud digiturvalisuse pädevuse enesehindamise küsimustik ja viis nende hinnangute kontrollimiseks.

Lõputöö eesmärk on sõnastada DigComp mudeli abil administratiivtöötajatele sobivad väited enesehindamisküsimustiku jaoks digiturvalisuse pädevuse valdkonnas ja testida enesehinnanguid situatsioonülesannetega. Autori hinnangul on administratiivtöö järjest enam liikumas digiruumi ja üha rohkem nõutakse administratiivtöötajatelt digiturvalisuse valdkonnas heade pädevuste omamist. Lõputöö eesmärgi saavutamiseks on autor püstitanud järgnevad uurimisülesanded:

- selgitada välja ja defineerida digiturvalise pädevuse mõiste ja põhimõtted;
- selgitada välja millised on digiturvalisuse teadmised, oskused ja hoiakud DigComp mudelis;
- kirjeldada empiirilise uuringu metoodika rakendamist;
- katsetada administratiivtöötajate digiturvalisuse pädevuse kontrollimiseks situatsioonülesanded;
- võrrelda DigComp mudeli põhise enesetaju ja digiturvalisuse pädevuse situatsioonülesannete lahendamise tulemusi.

2020. aastal koostatud OSKA ülevaade valdkonnaspetsiifilisest IKT- oskuste vajadusest toob välja lühiajalised (1 aasta) ja pikaajalised (5 aastat) nõuded administratiivtöötajatele (OSKA ülevaade valdkonnaspetsiifiliste IKT-oskuste vajadusest, 2020). Erinevas võtmes turvalist käitumist ja seadmete ning interneti kasutamist on välja toodud lausa kolmes oskuste kirjelduses, sh teadmised turvalisest kaugtöö lahendusest, virtuaalse suhtluse ja sotsiaalmeedia rakenduste turvalise kasutamise oskused ja teadmised digiturvalisusest, infoturbest ja andmekaitsest.

Käesolev lõputöö koosneb kolmest osast. Esimeses peatükis on kirjeldatud täiskasvanute digiturvalisuse pädevuse hetkeolukorda Eestis, selgitatud on digiturvalisuse mõiste, küberruumi olemus ja kirjeldatud seal valitsevaid ohte. Teises peatükis on kirjeldatud DigCompi mudelit ja riikliku digipädevuse mudelit ning nende kasutamist teistes valdkondades, sh õpetajate, lapsevanemate ja õpilaste hulgas. Kolmandas peatükis kirjeldab autor empiirilise uuringu metoodikat, viib läbi andmete analüüsi ja esitab järeldused ning soovitused edasiseks uurimiseks.

1 TÄISKASVANUTE DIGITURVALISUSE PÄDEVUSE OLUKORD EESTIS

Elukestva õppe strateegia 2020. vahehindamise teemalehes 06/19 on tõstatud küsimus: millised on praeguste täiskasvanute digipädevuste koolituste sihtgrupid ja eesmärgid? Inimeste tunnetuslikku digioskuste puudujääki, vajadust koolituse järele ning valmisolekut koolitustel osaleda ei ole uuritud ning selle kohta puudub ülevaade. Koolituste täpsemaks sihitamiseks võiks kaaluda täiskasvanud elanikkonna digioskuste koolitusvajaduse täpsemat kaardistamist (Digipööre hariduses ja uuenduslik õppevara, 2019). Erinevad avaliku- ja erasektori ettevõtted on kehtestanud oma sise-eeskirjades IKT testide läbimise nõude. Nii on näiteks kaitseministeeriumi valitsemisalas iga aastane IKT e-õpe ja test kõigile teenistujatele ja ametnikele kohustuslik. Kuid ka siin ei tegeleta mitte täiskasvanute digipädevuste kaardistamise ja koolitamise vaid süsteemse testimisega ning tähelepanu juhtimisega küberturvalisusele peamiselt töövaldkonnas. Siiski on IKT- seadmete kasutajad oma harjumuste ohvrid. Tavaliselt muutuvad inimesed ühel hetkel laisaks ega viitsi enam töö tegemiseks turvalist VPN-võrku tööle panna või unustavad paroole vahetada (Parve, 2021). Seda inimese vaimset nõrkust leevendab näiteks Apple oma seadmetel nii, et soovitab kasutajale väga keerukaid paroole rakenduste turvamiseks. Nende paroolisoovituste suurimaks miinuseks on see, et need on nii rasked ja juhuslikud, et nende meeldejätmine on ebatõenäoline ja selle tõttu pakub Apple veelgi mugavamalt *Keychain*-teenust, kus kasutaja paroolid salvestatakse pilve (Set up iCloud Keychain, 2022). Autori hinnangul muudab see kasutaja mugavaks, kuna paroolide meeldejätmine ei ole võimalik ja samas annab küberruumi turvalisuse selgelt üle füüsilise seadme turvalisusele, st kuniks seade on ohututes tingimustes (või Apple näitel seadmete perekond ja personaalne kasutajakonto), on ka küberruumis kasutaja turvatud.

Digiturvalisuse pädevuse algatusse panustab ka Kaitseliidu eriorganisatsioon Naiskodukaitse. Nende eestvedamisel loodi mobiilirakendus OLE VALMIS!, kus on võimalik läbida küberhügieeni alusõppe moodul. Läbides kõik õppetükid, on võimalik kõigil omandada paremad teadmised, kuidas ennast kaitsta küberruumist lähtuvate ohtude ja rünnakute eest (Naiskodukaitse, OLE VALMIS!). Rakenduses leiduv e-õpe sisaldab 16 õppetükki ja kogu e-õppe läbimine koos testidega võtab aega 45 minutit. Autorile teadaolevatel andmetel teist nii mahukat eesti keelset vabalt kättesaadavat küberhügieeni õppekeskkonda rohkem pole.

Haridus- ja Teadusministeeriumi (HTM) 2020. aastal loodud “Haridusvaldkonna arengukava 2021-2035” toob välja praeguse haridusvaldkonna olukorra kitsaskohad, sealhulgas täiskasvanute vähese

valmisoleku oma oskusi pidevalt täiendada ja tööandjate madala motivatsiooni oma töötajate oskusi, sh digioskusi arendada (Haridusvaldkonna arengukava 2021-2035). Tehnilisest tööst oluliselt raskem on aga kehtestada uusi tööpõhimõtteid või selgitada inimestele, kuidas informatsiooni turvaliselt käidelda (Parve, 2021). Tehnoloogia abil saame oma küberruumi kaitsta ligikaudu 80% ulatuses, aga ülejäänu on inimese kätes ja inimene on ekslik (Palm, 2021). Seega tuleb lisaks tehnoloogiliste seadmete ja tarkvara hindamisele pidevalt tegeleda ka töötajate koolitamise ja arendamisega. Nii pakub Töötukassa tööandjatele võimalust küsida toetust töötajate digioskuste arendamiseks. Töötukassa vaates ei näe „madalama digioskuste tasemega inimesed sageli [...] vajadust midagi juurde õppida, kuna senine kokkupuude digilahendustega on olnud napp“ või teisalt hinnatakse oma võimeid igapäevaeluga toimetulekul piisavaks (Tööandjad saavad uuest aastast toetust töötajate digioskuste arendamiseks, 2020). Autori hinnangul on digiühiskond ja sealhulgas ka digiturvalisus igapäevases arengus ning selles valdkonnas peaks iga kodanik end süsteemselt harima.

Euroopa Komisjon digitaalmajanduse ja -ühiskonna indeks võtab kokku Euroopa digitaalse jõudluse näitajad ja jälgib ELi riikide edusamme (The Digital Economy and Society Index (DESI)). 2021. aastal korrigeeriti DESI ülesehitust ning aruanne koosneb nüüd neljast EL digikompassi osast: inimkapital, ühendatus, digitehnoloogia integreerimine ja avaliku sektori digiteenused. Digitehnoloogia kasutusele võtmisel on Eesti ettevõtetes märkimisväärne potentsiaal veel kasutamata (Euroopa Komisjon, 2021). Autori hinnangul tähendab digitehnoloogia suurem kasutusele võtt seda, et ettevõtted peavad läbi mõtlema oma turvastrateegiad ja tegema need mõistetavaks oma töötajatele, muu hulgas järjepidavalt koolitama ja kontrollima keskselt strateegia täideviimist.

1.1 Digiturvalisuse mõisted

RIA, Majandus- ja Kommunikatsiooniministeerium (MKM) ja paljud teised organisatsioonid kasutavad läbivalt mõistet „küberturvalisus“ (*cyber security*), selgitades, et „küberturvalisus on seisund, kus kõikvõimalikud ohud, mis võiksid mõjutada digitaalseid andmeid ning arvutite, nutiseadmete, mälupulkade ja samuti e-teenuste kasutamist, ei realiseeru“ (Himma, 2018). Autori hinnangul on küberturvalisuse põhimõtteid võimalik edukalt kanda üle individuaalse digipädevuse konteksti, kuid seda valdavalt ettevõtte tegevuse planeerimise valdkonnas. Näiteks on RIA ettevõtte juhtidele koostanud „Ettevõtte küberturvalisuse lühijuhendi” mille sisu on mõeldud selleks, et aidata ettevõtetel astuda esimesi samme küberturvalisemate äriprotsesside suunas (Ettevõtte küberturvalisuse lühijuhend, 2019). Üheks suureks teguriks kaasajastatud infotehnoloogilistele vahendite kõrval küberturvalisemate äriprotsesside saavutamiseks ettevõttes on ettevõtte töötajad ja

nende teadmised turvalisemast küberkäitumisest. Autori hinnangul läbimõeldud küberturvalisuse strateegia toetab ja suunab iga töötaja küberkäitumist, kuid ei elimineeri inimfaktorist tingitud vigu.

Varasem küberruumis kasutusele võetud internetiohtudega tegelev mõiste on ehk „infoturve“ või „infoturvalisus“ (*information security*). See on „teabe konfidentsiaalsuse, tervikluse ja käideldavuse säilitamine“ ([ITS] IT terministandardi sõnastik). Autori hinnangul on infoturve indiviidi seisukohast veidi kauge mõiste keskendudes peamiselt asutuste ja ettevõtete vastutusele kaitsta nende poolt kogutud andmeid. Üheks suuremaks privaatsusega seotud infoturbe regulaatoriks on nt isikuandmete kaitse määruse (*General Data Protection Regulation, lühend GDPR*) leping Euroopas, mis võeti vastu 2018. aastal, et ühtlustada EL andmekaitseõigusi. Regulatsiooni eesmärk on anda tavakasutajale võimalus näha, milliseid andmeid tema kohta koguda soovitakse ning nende kogumisega nõustuda või keelduda. Autori hinnangul on GDPR mõjutanud oluliselt veebikülgede kasutusmugavust ja tavakasutajate vähene motivatsioon elektrooniliste kokkulepete mõistmiseks (nt veebipoe lepingute või küpsiste ehk *cookies* sätetega nõustumine) loob täiendavad võimalused küberruumi ärakasutamiseks nii eetiliselt kaheldavatel ärilistel kui ka kuritegelikel eesmärkidel.

Majandusliku Koostöö ja Arengu Organisatsioon, (*Organisation for Economic Co-operation and Development*, OECD), mille liige on Eesti alates 2010. aastast, on seisukohal, et kaasaegses, avatud ja läbipõimunud digimaailmas on sotsiaal- ja majandusvaldkonna arenguks vaja tagada asjakohane reeglistik (seadusandlus) digiturvalisusele. Kui küberturvalisus keskendub pigem tehnilistele teguritele siis digiturvalisus on laiapõhjalisem ja sisaldab ka majanduslike ja sotsiaalseid tegureid (OECD).

Täiendavalt on eesti keeles ametlikult kasutusel terminid „küberhügieen“ ja „digihügieen“, mida defineeritakse kui „riigi, asutuse, inimese teadlikku tegevust oma digiseadmete ja elektrooniliste andmete kaitsmiseks” (Sõnaveeb). Autori hinnangul on selline määratlus kitsam kui käesoleva lõputöö jaoks vajalik, sest küberhügieeni mõiste haarab vaid kitsast osa digiturvalisusest.

Digiturvalisus *(digital safety)* on „isiku heaolu, privaatteabe ja varade kaitstus digitaalses võrgukeskkonnas“ (Sõnastik). Autori hinnangul on küberturvalisuse sisu tehnilisem, digiturvalisus aga laiapõhjalisem ja hõlmab endas lisaks ka sotsiaalset ja keskkonna mõõdet. Käesoleva lõputöö raames kasutab autor läbivalt digiturvalisuse pädevuse mõistet järgneva definitsiooni alusel: digiturvalisuse pädevus tähendab inimese käitumist küberruumis ja IKT seadme kasutamisel selliselt, et ta ei sea ohtu privaatelu turvalisust, organisatsiooni turvalisust, enda tervist ega teda ümbritsevat keskkonda.

1.2 Digiturvalisuse pädevuse sobitumine küberruumi

MKM koostatud arengukavaga „Eesti digiühiskond 2030“ on paika pandud kindlad suunad, milleni soovitakse 2030. aastaks jõuda. Kolmeks suurimaks alaeesmärgiks on arengukavas välja toodud digiriik, ühenduvus ja küberturvalisus. Küberturvalisuse eesmärkideks 2030. aastaks on ajakohane küberturvalisuse riiklik korraldus, suundumuste, riskide ja mõjude analüüsivõime ning suurem küberturvalisuse tagamise võimekus (Eesti digiühiskond 2030, 2021). Autori hinnangul on senini jäänud riiklikud regulatsioonid pettustega seotud küberruumi intsidentidele puudulikuks. Näiteks ei ole pärast investeerimispettuste ilmsiks tulemist petta saanud isikul mingit lootust raha tagasi saada ning petturitki ei ole sageli suudetud vastutusele võtta.

Justiitsministeeriumi 2020. aasta kokkuvõttes on küberkuriteod olnud tõusujoones. Samal aastal läbi viidud ohvriuuring näitas, et inimeste kokkupuuted arvutiõngitsemiste jms on sagenenud – sellega kokku puutunuid oli 52%, mis on 12% rohkem kui 2019. aastal (Küberkuriteod). Tõenäoliselt jäävad paljud sotsiaalmeedia kuriteod registreerimata, sest ohvrid ei tea, et tegu on ühe kuriteo liigiga ning häbenetakse oma oskamatust. Enamasti on sotsiaalmeedia veebikonto paroolide muutmise ohvrid naised (56%), kelle keskmine vanus on 36 aastat (Küberkuriteod). Autori arvates on ühiskonna digitaalne toimepidevus seega seotud tugevalt iga indiviidi isikliku pädevusega osata märgata ja end kaitsta küberkuritegude vastu.

Eesti osales perioodil 2008-2015 rahvusvahelises täiskasvanute oskuste (*Programme for the International Assessment of Adult Competencies,* PIAAC) uuringus. Uuringu eesmärk oli mõõta laiapõhjalisi infotöötluse oskusi neljas kategoorias:

- funktsionaalne lugemisoskus;
- matemaatiline kirjaoskus;
- probleemilahendusoskus tehnoloogiarikkas keskkonnas;
- lugemise ja arvutamise baasoskused.

Tegemist on oskustega, mis on eduka toimetuleku aluseks nüüdisaegses infoküllases ühiskonnas (Infotöötlusoskused ja näidisülesanded, 2021). Eesti täiskasvanute arvutikasutusoskuse ja –julguse ning tehnoloogiarikkas keskkonnas probleemilahendusoskuse tase on oodatust madalam. Heade ja väga heade probleemilahendusoskustega on vaid iga neljas täiskasvanu. 30% ei oska või ei julge uut tehnoloogiat kasutada (Rahvusvaheline täiskasvanute oskuste uuring PIAAC). Autori hinnangul ei eristu tänased administratiivvaldkonna töötajad olulisel määral tavakasutajatest, mistõttu võib

uuringu tulemusi üle kanda ka administratiivtöötajatele. Aastatel 2018-2024 toimub PIAACi kordusuuring, kus Eesti valimis osaleb ligi 3800 inimest (Haridus- ja Teadusministeerium, 2021).

RIA "Trendid ja tähelepanekud küberruumis - I kvartal 2022" toob välja Eesti hetkeolukorrast neli teemat, millest üks puudutab küberründeid. Väga palju proovitakse e-kirja teel levitada pahavara, enamasti trooja hobuste (viiruse liik) erinevaid variatsioone, mis sisalduvad meiliga kaasas olevas dokumendis ja käivituvad selle avamisel. Selliseid laineid on nähtud ka varasemalt, ent praegused mahud on tavapärasest suuremad. Mõnel juhul on peibutisena kasutatud sõjaga seonduvaid teemasid, ent rohkem liigub varasemast tuttavaid teemasid (arve, hinnapakkumine jne) (RIA, 2022). Autori hinnangul on küberründed seda edukamad, mida nõrgem on elanikkonna digiturvalisuse pädevus, sh mängib oht küberründeks eriliselt suurt rolli administratiivtöötajate võrgustikes, kes sageli pääsevad ligi ka sensitiivsele infole. Ühe administratiivtöötaja töökeskkonna kaaperdamine võib omada laiapindsemat mõju, kui sarnane intsident kooliõpilase digikeskkonnas.

2 DIGCOMPI MUDEL JA RIIKLIK DIGIPÄDEVUSE MUDEL

2006. aastal toodi välja EL tasandil kaheksa elukestva õppe võtmepädevust. Nendeks on emakeeleoskus, võõrkeeleoskus, matemaatikapädevus, teadmised teaduse ja tehnoloogia alustest, digipädevus, õppimisoskus, sotsiaalne ja kodanikupädevus, ettevõtlikkus ning kultuuriteadlikkus ja -pädevus (Ferrari, 2013). Tehnoloogia kiire areng on viinud järelduseni, et sellises ühiskonnas jätkusuutlik elamine nõuab ka tehnoloogia tundmist ja kasutamist. Digimaailmas osalemine ei ole enam „osalen või ei osale“ küsimus, vaid on pigem seotud „peab osalema“ põhimõttega (Ferrari, 2013). Autori hinnangul tuleb seega administratiivtöötajate kutse omandamisel järjest suuremat tähelepanu pöörata digipädevuste omandamisele eriti just digiturvalisuse valdkonnas.

DigComp mudel sündis Euroopa Komisjoni kolme erineva valdkonna vajadusest ühtlustada oma senist tõlgendust digipädevusest ja selle hindamise viisidest. Haridus- ja kultuuri peadirektoraadi, tööhõive, sotsiaalküsimuste ja sotsiaalse kaasatuse peadirektoraadi ning infoühiskonna ja meedia peadirektoraadi digipädevuse käitlused võeti kokku, et neist siis luua kõigile sobiv ühine raamistik. Projekti käigus loodi digipädevuse enesehindamisvahend ja mudel, milles kirjeldatakse detailselt digipädevuse olemust (Ferrari, 2013). Autor leiab, et digipädevuse hindamiseks ainult enesehinnangust ei piisa kuivõrd esineda võib soovmõtlemist, iga indiviidi enesetaju ning hindamisküsimuse tõlgendamine võib olla märkimisväärselt erinev. Lisaks seavad enesehindamisküsimustikele vastamisel piirangud iga organisatsiooni turvastrateegiad. Näiteks on organisatsioone, kus töötaja ei saa ise mitte ühtegi uut tarkvara/programmi alla laadida vaid peab selleks pöörduma IT- osakonna poole.

Enamus DigComp enesehindamisküsimustike arendusi ja digioskuste parandamise keskkondi on suunatud õpilastele ja õpetajatele. Seda põhjusel, et just õppekeskkondades on kõige suurem võimalus veel uusi oskuseid ja harjumusi juurutada. DigCompi enesehindamisvahendit ja mudelit on erinevates Euroopa maades kasutusele võetud väikeste erinevustega. Taani „ *The Digital Competence Wheel“* eesmärk on pakkuda ülevaade küsimustikutäitja digipädevustest, anda ideid ja pakkuda lahendusi digipädevuste arendamiseks (Digipädevus maailmas). Autor leiab, et enesehindamise olulisem funktsioon seega võib olla tähelepanu tõmbamine olulistele teemadele, millele administratiivtöötajad ehk sageli ei mõtle.

Kaitseministeerium ja Tallinna Tehnikaülikooli Küberkriminalistika ja -julgeoleku keskus on koostanud KüberPähkli uuringu ja testimise õpilastele, mille põhieesmärgid on erinevate digitaalse ohutuse ja küberkaitse alasete teadmiste uurimine, testimine ja lahenduste leidmine. 2018. aastal viidi

uuring läbi avalikult kasutades DigComp enesehindamisküsimustiku ning vastata said kõik alates 10. eluaastast. Uuringus kasutati enesehinnangu vormi, millega hinnati digikasutuse valdkonna oskusi ja milliseid lahendusi oskuste parendamiseks kasutatakse. Lisaks kaardistati vastanute harjumused ja oskused digitaalse ohutuse ja küberkaitse teemades: privaatsus ja turvalisus, tehniline taiplikkus, kriitiline mõtlemine ja sotsiaalne manipulatsioon, käitumine ja hoiakud riigi tegevuse suhtes eriolukorras, ootused koolitusteks (Birgy, Sõmer, Osula, Ääsmäe & Üürike, 2018). Autori hinnangul on administratiivtöötajatele sarnaste ettepanekute tegemiseks esmalt vaja uurida, milline on hetkeseis selle sihtgrupi digiturvalisuse pädevuse valdkonnas.

Uuringu kokkuvõttes on välja toodud soovitused täiskasvanute harimiseks:

- luua täiskasvanud õppijatele toetav veebileht. Kui lastele, lapsevanematele ja õpetajatele on programm „Targalt internetis“, siis täiskasvanutele, kes sinna sihtrühma ei kuulu, pole oma keskset veebipesa, et arusaadavas lihtsas keeles abi saada, uudiseid lugeda, teste teha ja oma küberhügieeni alastes oskustes veenduda (et turvaliseks käitumiseks ei pea ilmtingimata teadma, tehnilist terminoloogiat);
- luua koolitusprogramm või e-kursus, mida saab inimene või tööandja kasutada oma töötajate koolitamiseks. Kõige lihtsam on teha ennetustööd inimestega, kes on veel haridussüsteemis – koolis, ülikoolis, kutsekoolis või osalevad koolitustel. On vaja tekitada formaalseid ja mitteformaalseid õppimisvõimalusi täiskasvanutele, kes enam haridussüsteemis ei ole;
- märgata erinevaid sihtrühmi ja vajadusi ühiskonnas (vanemad inimesed, vähese digioskusega inimesed). Kõik ei pea olema küberhügieenis samal tasemel, aga kõikidel peaks olema saavutatud vähemalt baasoskuste tase. Kuna täna puudub arusaam, mis on baastase ja mis on selle järgnevad astmed praktilisel skaalal, siis tuleks kõigepealt luua vastava hierarhiaga maatriks ning selle alusel luua teste, materjale, aga ka koolitusi;
- kasutamata ressurss on tööandja poolsed koolitused tavalisele töötajale, eriti oluliseks peetakse avaliku sektori pädevust antud vallas (Birgy, Sõmer, Osula, Ääsmäe & Üürike, 2018).

Autori hinnangul on kokkuvõttes väljatoodud soovitused vajalik teostada, et e-riik saaks veel paremini toimida ja mitmed ettepanekud ei ole teostatavad individuaalsel tasemel. Sagedamini peaksid ka organisatsioonid sisekoolitusel tähelepanu pöörama digiturvalisuse valdkonnale.

Eestis on õpetajate ja õpilaste digipädevuse arendamise eest vastutav Haridus- ja Noorteamet. Selleks on loodud eraldi keskkond www.digipadevus.ee, kuhu on koondatud õpetajate ja õpilaste digipädevuse mudelid. Käesoleva uurimustöö raames kirjeldatakse vaid õppija digipädevuse mudelit, kuna autori hinnangul peavad administratiivtöötajad lähtuma oma töökohustusi täites ka

kutsestandardist (nt Sekretär, tase 5 ja Juhiabi, tase 6 kutsestandardid). Seetõttu on võimalik administratiivtöötajatele rakendada digipädevuse mudeli õppija kutsehariduse astme hindamiskriteeriumeid. Digipädevuse mudel on jaotatud viieks valdkonnaks ja need omakorda jaotuvad pädevusteks, millest enamus on sõnastatud „teab, oskab“ formaadis (Lisa 3). Digipädevuse viis valdkonda on: info ja andmekirja oskus, suhtlus ja koostöö digikeskkonnas, digisisu loomine, digiturvalisus ja probleemilahendusoskus. Kõik viis valdkonda jagunevad omakorda pädevusteks. Pädevusi on kokku 21 ning need omakord jagunevad kolme pädevustasemesse: A- algaja, B- kesktase ja C- edasijõudnu (Ferrari, 2013).

Vastavalt õpieesmärkide taksonoomiale (Bloom, Engelhart, Furst, Walker & Krathwohl, 1956) tuleks oskuste, teadmiste ja hoiakute sõnastamisel lähtuda põhimõttest, et pädevuse kirjeldus peab väljendama silmaga nähtavat või ettekujutatavat sooritust, mida õppur või töötaja teeb. Näiteks on mõistlik sõnastada „teab GDPR põhimõisteid“ viisil, mis väljendaks tegevust - nagu „selgitab GDPR põhiolemust terminoloogiliselt korrektselt“. Eelnevast tulenevalt ei ole autori hinnangul administratiivtöötajate väidetel põhinevate enesehindamise küsimuste koostamine Eesti digipädevuse mudeli III, IV ja kutsehariduse tasemelt ilma ümber sõnastamata kasutatavad, mistõttu käesoleva lõputöö raames tuleb luua selgem sümbioos DigComp mudeliga. Siinkohal on oluline märkida, et õpieesmärkide taksonoomiat tõlgendatakse sageli ekslikult kui Bloomy taksonoomiat, mis käsitleb vaid kognitiivset (teadmistel põhinevat) õpidomeeni. Autor on seisukohal, et digipädevuste hindamisel peab arvestama aga kõigi kolme – so kognitiivse (teadmised), psühhomotoorse (oskused) kui ka afektiivse (hoiakud) domeeniga - ja seda ka DigComp teoreetiliselt võimaldab.

Märtsis 2022. aastal uuendati DigComp mudelit (DigComp 2.2). Parandatud mudelis on juurde toodud neljas pädevustase (spetsialist) ning iga pädevustaset on täpsustatud omakorda kahe väitega. Kokku on kõigi pädevusvaldkondade peale kirjeldatud 250 oskust, teadmist ja hoiakut (Vuorikari, Kluzer, & Punie, 2022). Tulenevalt dokumendi avaldamise ajastusest DigComp 2.2 käesoleva lõputöö raames ei kasutatud, olgugi, et autori hinnangul on tegemist oluliselt täiendatud versiooniga mudelist, mille kasutegur sarnaste uurimuste läbiviimisel oleks oluliselt tõhusam.

3 EMPIIRILISE UURINGU METOODIKA

Lõputöö eesmärk on sõnastada DigComp mudeli abil administratiivtöötajatele sobivad väited enesehindamisküsimustiku jaoks digiturvalisuse pädevuse valdkonnas ja testida enesehinnanguid situatsioonülesannetega. Uurimisprobleemiks on, et puudub administratiivtöötajatele kohandatud digiturvalisuse pädevuse enesehindamise küsimustik ja viis hinnangute kontrollimiseks.

Kasutajate teadlikkuse kasvatamise ja ohutu küberkäitumise normide juurutamisega tuleb pidevalt tegelda ja selle tulemusi regulaarselt mõõta (Kaitseministeerium). Käesolev uurimus on ühekordne, et selgitada välja kuivõrd erineb enesetaju ja praktilised oskused, kuid pikemaajalist uurimise järgset mõju ei hinnata, hoolimata sellest, et selline mõju on olemas.

Uurimuse populatsiooni moodustavad administratiivtöötajad. OSKA raporti järgi kuuluvad ühise nimetuse alla (administratiivtöötajad) järgnevad kutsealad: üldsekretärid, administraatorid, teabe- ja dokumendihaldurid, sekretärid, juhiabid, büroojuhid, infotelefoni töötajad ja andmesisestajad. Sellisele profiilile vastab OSKA raporti järgi 2011. aasta rahvastiku- ja eluruumi loenduse andmetel 22000 töötajat (Kutsekoda, 2018). Valimi moodustamisel võttis autor aluseks, et sotsiaalteaduslike uuringute läbiviimisel on trendide kaardistamiseks piisav usaldusnivoo 95% (Õunapuu, 2014). Käesoleva uurimistöö raames peaks valimi moodustama seega 10% veapiiriga 96 vastajat. Autor on teadlik, et väikese vastajate hulga korral ei ole võimalik kogu populatsioonile kehtivaid järeldusi esimese ja teise uurimisküsimuse puhul teha.

Valimi puhul on tegemist mugavusvalimiga, mida ilmestab uuringus osalemise kutse jagamise viis. Mugavusvalimi puhul lähtutakse lihtsa kättesaadavuse, leitavuse ja uuritavate koostöövalmiduse põhimõtetest (Õunapuu, 2014). Autor edastas uuringus osalemise kutse e-mailitsi Võru maakonna kohalikesse omavalitsustesse. Lisaks jagas autor uuringus osalemise kutset sotsiaalmeedia keskkonnas Facebook järgnevatel lehtedel ja gruppides:

- Eesti Juhi Abi Ühing (170 jälgijat);
- Dokumendihaldurid (1400 liiget);

Veebi teel läbi viidud uuringute suurimaks puuduseks peetakse valimi halba kättesaadavust (kutse uuringus osalemise kohta võib mattuda infomüra alla, liigituda rämpsposti). Tavapärasele lisaks on seoses Ukraina sõjakriisiga olulisel määral suurenenud ametnike töökoormus, samuti võib suurema küberründe ohu tõttu olla administratiivtöötajate organisatsioonides varasemast rangem turve. Sotsiaalsuhtluskeskkonna kaudu oli uuringus osalejatel võimalik ka küsimustiku kohta personaalselt küsimusi esitada ja arvamust avaldada.

Autor lähtus uurimistöö kavandamisel vajadusest koguda esmaseid andmeid administratiivtöötajate digiturvalisuse digipädevuse kohta, kuna selliseid andmeid varasemalt Eestis kogutud ei ole. Andmete kogumiseks kasutas autor veebiküsitluse formaati Google Forms keskkonnas, kuna see on vabavaraliselt kättesaadav, lihtsasti vastajatega jagatav ning lihtsasti kohandatav. Andmed on kogutud anonüümselt ja tunnuste avaldamine ei võimalda uuringus osalejate isikustamist. Andmed hoiustatakse Google Drive keskkonnas.

Andmete töötluseks kasutas autor Microsoft Excel tabelarvutusprogrammi statistikaliidest (*data analysis module*) ja Pivot moodulit. Seoste leidmisel kasutas autor SPSS Statistics tarkvara.

3.1 Enesetaju küsimustiku koostamine ja tõlgendamine

Küsimustik koosneb kahest osast. Esimeses osa koostamise aluseks võttis autor DigComp mudeli, milles on esitatud väited „mina"-vormis. Väited on esitatud igas alapädevuses A (algaja), B (kesktase) ja C (edasijõudnu)- tasemel (*proficiency level*) ehk pädevustasemed ning autor muutis nende sõnastust vaid sellises ulatuses, mis võimaldaks vastajal sõnapeensustesse süvenemata eristada küsimusi teineteisest, kuid mitte eristada oskuste taset, millele see väide võiks vastata. See tähendab, et vastajatel puudub teadmine, millise oskustaseme väitega on tegemist. Kuna mõni väide oli pikk ja koosnes mitmest komponendist, siis muutis autor ühe väite mitmeks väiksemaks ja selgemini arusaadavamaks. Kõik väited on esitatud suvalises järjestuses, kuid kohati võib esineda sarnaste küsimuste grupeerumist. Küsimused on koostatud vaid digiturvalisuse pädevusi silmas pidades, olgugi, et ka teised digipädevuse kategooriad kaudselt mõjutavad digiturvalist käitumist.

Küsimustikus on esitatud 36 väidet, millele uuringus osalejad vastavad lähtuvalt enesehinnangust, mil määral väide nende kohta kehtib. Hindamisvahemik on üles ehitatud reitinguskaalal 5-palli süsteemis, kus „5" iseloomustab alati ja „1" ei iseloomusta üldse. Reitinguskaalaga annab vastaja hinnangu küsimusele/väitele, lähtudes skaala punktide väärtusetest (Õunapuu, 2014).

Teises osas esitab autor küsimused kategoriseerimiseks hariduse, elukoha, vanusegrupi, ja varasemalt läbitud digiturvalisuse alase õppe/koolituse järgi. Haridustase võimaldab mõista enesetaju seoseid varasemalt läbitud haridusteega. Vanusegrupp võimaldab hinnata ühiskonna digitaliseerimisest tingitud mõjusid tööjõule. Lisaks küsib autor uuringus osalejatelt, kas nende töökoht on era- või avalikus sektoris, kuivõrd eelduslikult peaks avaliku sektori digivaldkond olema tsentraliseeritum ja seetõttu avalduma vastustes. Just avaliku sektoris töötatavatelt administratiivtöötajatelt tuli enesehinnanguküsimustiku täitmisel täiendavaid küsimusi. Näiteks väide „Ma lülitan töölt lahkudes arvuti välja" on Kaitseministeeriumi ja Siseministeeriumi valitsemisalas

olevatel töötajatel keelatud kuna nende IKT valdkonna spetsialistid teevad just ametnike töö välisel ajal programmi- ja seadmehooldus töid distantsil ning selleks on vaja, et seadmed oleksid võrgus (lukustatud kuid puhke režiimil).

Tärniga tähistatud pädevuse väited on lisaküsimused, mille vajalikust pidas autor antud uuringus tähtsaks. Väited „Ma olen teadlik oma ettevõtte/organisatsiooni turvastrateegiast“ ja „Ma järgin oma ettevõtte/organisatsiooni turvastrateegiat“ näitavad autori hinnangul organisatsiooni mõju administratiivtöötaja digiturvalisuse pädevuse enesehinnangule.

3.2 Situatsioonülesannete kasutamine empiirilises uuringus

Situatsioonülesannete eesmärk on enesehindamisküsimustiku ja praktiliste oskuste kõrvutamine. Uuringus autor kasutas juba olemas olevaid ja varasemalt testitud situatsioonülesandeid (v.a situatsioonülesanne 4, mille koostamisel kasutati enesehinnangupädevuste loendit). Kasutuses on kaks Tartu Ülikooli digipädevuse enesetesti kaitstuse küsimust ja üks situatsioonülesanne Küberkaitse gümnaasiumi valikõppeaine veebiraamatust. Varasemalt testitud situatsioonülesannete sobivust administratiivtöötajate digiturvalisuse pädevuse kontrollimiseks kasutati samuti enesehinnangupädevuste loendit. Situatsioonülesandeid asuvad küsimustiku lõpus ja ülesanded näitavad nelja erinevat digiturvalisuse pädevuse oskust (Lisa 2).

Tabel 1. Digiturvalisuse pädevuse väidete jaotumine situatsioonülesannete vahel (Ferrari, 2013)

Situatsioon ülesande nr ja sisu	Mitut digiturvalisuse enesehinnangu pädevust antud situatsioonülesanne testib ?	Digiturvalisuse enesehinnangu pädevused
Situatsioonülesanne 1 näitab kui hästi on vastajaid kursis erinevate keskkondade kasutajatingimustega	6 digiturvalisuse enesehinnangupädevust	1. Ma saan privaatsuse küsimustest üldiselt aru 2. Ma tean, et ma tohin enda ja teiste kohta e-keskkondades jagada ainult teatavat tüüpi infot 3. Ma oskan kaitsta enda ja teiste privaatsust e-keskkonnas 4. Ma olen privaatsusküsimustega kursis, mul on selles valdkonnas laiad teadmised 5. Ma tean, kuidas asutuses andmeid säilitatakse ja mis privaatsuspõhimõtteid rakendatakse 6. Ma tean, kuidas minu andmeid kogutakse ja kasutatakse

Situatsioonülesanne 2 testib vastajate arusaama digitehnoloogia kasutamisest ja käitlemisest tekkivast tervise- ja keskkonna ohust	11 digiturvalisuse enesehinnangupädevust	1. Ma tean, et tööalaselt kasutatavad tehnoloogilised vahendid võivad tekitada sõltuvust, kuna neil on ka teisi kasutusotstarbeid 2. Ma uurin enne seadmete väljavahetamist töökohal, millised on parimad saadaolevad tehnoloogilised seadmed ja tarkvara 3. Ma lülitan töölt lahkudes arvuti välja 4. Ma mõistan, et minu vajadused uute seadmete järele võivad mõjutada keskkonda 5. Ma tean, kuidas kasutada tehnoloogilisi vahendeid nii, et vältida terviseprobleeme 6. Ma tean, kuidas leida hea tasakaal e-maailma ja füüsilise maailma vahel 7. Ma olen teadlik tehnoloogia mõjust igapäevaelule, veebitarbimisele ja keskkonnale 8. Ma tean, et tehnoloogiliste vahendite väärkasutus võib kahjustada minu tervist 9. Ma kasutan põhivõtteid energia säästmiseks 10. Mõistan tehnoloogiliste vahendite kasutamisega seotud terviseriske (alates ergonoomika aspektidest kuni tehnoloogiasõltuvuseni) 11. Ma saan aru tehnoloogia kasutamise positiivsest ja negatiivsest mõjust keskkonnale
Situatsioonülesanne 3 tuleb vastajal hinnata parooli tugevust	5 digiturvalisuse enesehinnangupädevust	1. Minu tööarvuti on kaitstud tugeva salasõnaga ja ainult mina saan seda kasutada 2. Ma oskan kasutada põhivõtteid oma seadmete kaitsmiseks (nt viirusetõrje, salasõnad jms) 3. Ma olen teadlik oma ettevõtte/organisatsiooni turvastrateegiast.* 4. Ma järgin oma ettevõtte/organisatsiooni turvastrateegiat.* 5. Ma kontrollin sageli oma turvasätteid ja -meetmeid
Situatsioonülesanne 4 testib vastaja oskust kaitsa end küberründe ohtude vastu	10 digiturvalisuse enesehinnangu pädevust	1. Ma tean, kellega võimalike probleemide korral ühendust võtta 2. Ma olen teadlik oma ettevõtte/ organisatsiooni turvastrateegiast* 3. Ma tean, kuidas oma digiseadmeid kaitsta 4. Ajakohastan oma turvastrateegiaid, sh varundan oma tööfaile 5. Ma järgin oma ettevõtte/organisatsiooni turvastrateegiat* 6. Ma kontrollin sageli oma turvasätteid ja -meetmeid 7. Kui ma installin internetist tarkvara oma tööarvutisse, siis kasutan tarkvara, mis kontrollib faili enne allalaadimist 8. Ma oskan rakendada meetmeid, kui mu seade on ohus 9. Ma tean, kuidas vältida küberkiusamist 10. Ma kasutan alati kaheastmelist autentimist

3.3 Andmete analüüsi meetod

Autor kasutab kvantitatiivseid analüüsi meetodeid kuna enesehindamise küsimustiku ja situatsioonülesannete vastused on kasutatavad binaarsete või järjestustunnustena. Nt vastajate hariduse tunnuse puhul on magistriharidus kõrgeima väärtusega ehk „6“ ja keskharidus madalaima väärtusega ehk „1“. Autor kasutab peamiselt tunnuste kirjeldavat statistikat ja Spearmani korrelatsioonikordajat (r). Spearmani korrelatsioonikordajaga saab mõõta seost kahe arvulise või pikema skaalaga järjestustunnuse vahel (Rootalu, 2014). Kõik vastused teisendati arvskaaladele selliselt, et nad oleks samasuunalised enesehindamisküsimustikuga. Binaarsete vastuste puhul, sealhulgas situatsioonülesannete õigete vastuste puhul „jah/õige“ teisendati arvule „2“ ja valede vastuste puhul „ei/vale“ arvule „1“. Autor hindas positiivsemaks väärtuseks (hinne „4“) lähiminevikus toimunud koolitust ja negatiivsemaks (hinne „1“) koolituse mitteläbimist. Meetodi plussiks on, et see võimaldab kirjeldada nii seose suunda kui ka seose tugevust. Meetodi miinuseks on, et äärmuslikud vastused võivad kallutada seose olemust (Rootalu, 2014). Kallutatuse vähendamiseks kontrollib autor kahtluse korral seose tõesust standardhälbega. Sotsiaalteaduste puhul võib küllaltki tugevaks seoseks pidada juba korrelatsioonseoseid tugevusega (absoluutväärtuselt) üle 0,5 (Rootalu, 2014). Käesoleva uurimustöö käigus kirjeldab autor keskmiseid ja tugevaid korrelatsiooniseoseid ning mõnede üldlevinud seoste puudumist (nt: vanus ja kõrge enesehinnangu tulemused).

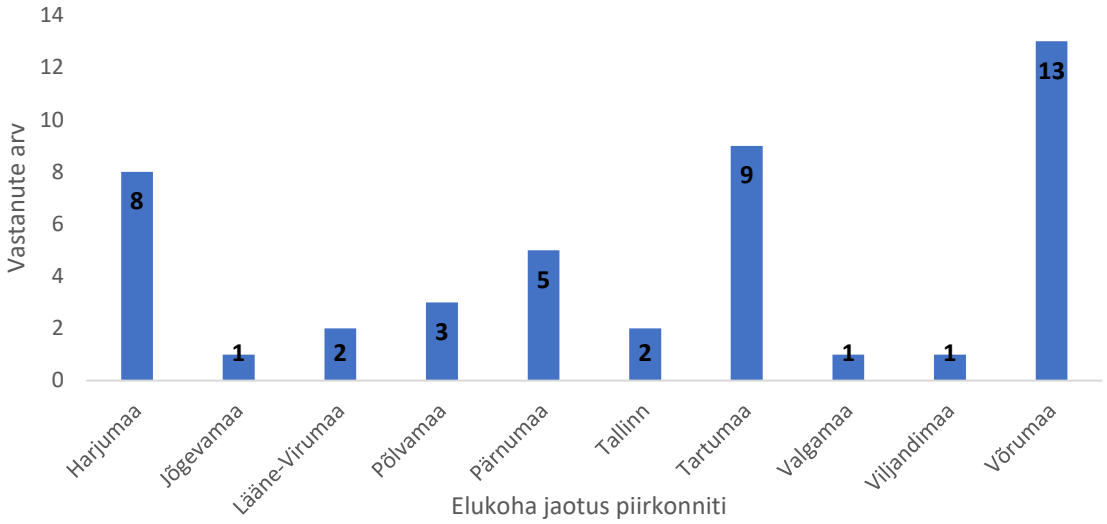
Kirjeldav statistika võimaldab kogutud andmete tunnuste tüüpide järgi analüüsimist. Lisaks kasutatakse tunnuste kirjeldavas statistikas sagedustabeleid ja standardhälvet. Tõenäoliselt kõige sagedamini kasutatav näitaja statistilises andmete analüüsis on aritmeetiline keskmine ehk keskväärtus ning standardhälve (SD), mis iseloomustab vastuste hajuvust keskmise ümber (Rootalu, 2014).

Kompetentside keskmiste arvutamisel on koondatud väited pädevustasemete kaupa tabelitesse. Digiturvalisuse pädevus on jagatud nelja kompetentsi: seadmete kaitse, isikuandmete kaitse, tervise kaitse ja keskkonna kaitse. Iga väite kohta on arvutatud aritmeetiline keskmine ja standardhälve.

3.4 Uuringu tulemused

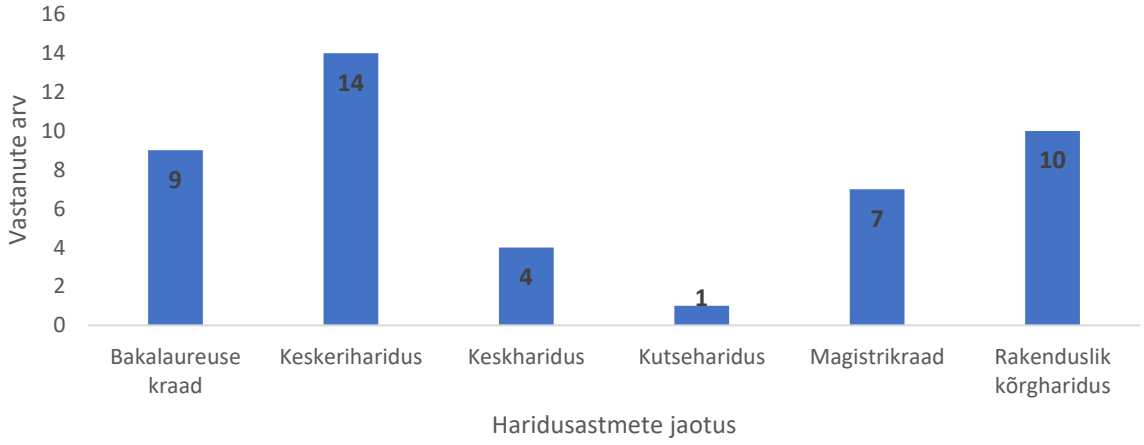
Uuringus osales 45 vastajat, mis 95% usaldusnivoo korral tähendab veapiiri 15%, mistõttu uuringu tulemuste ülekandmine populatsioonile ei ole eesmärgipärane ja kirjeldab pigem võimalikku trendi kui tegelikkust. Seega on käesoleva uuringu tulemused ja analüüs kasutatavad vaid antud lõputöö raamistikus.

Esmalt analüüsime sotsiaal demograafilisi andmeid, et hiljem tuua välja seosed väidetega mille korrelatsioonikordaja näitab tugevat või keskmist seost.



Joonis 1. Uuringus vastanute elukoha järgne jaotus

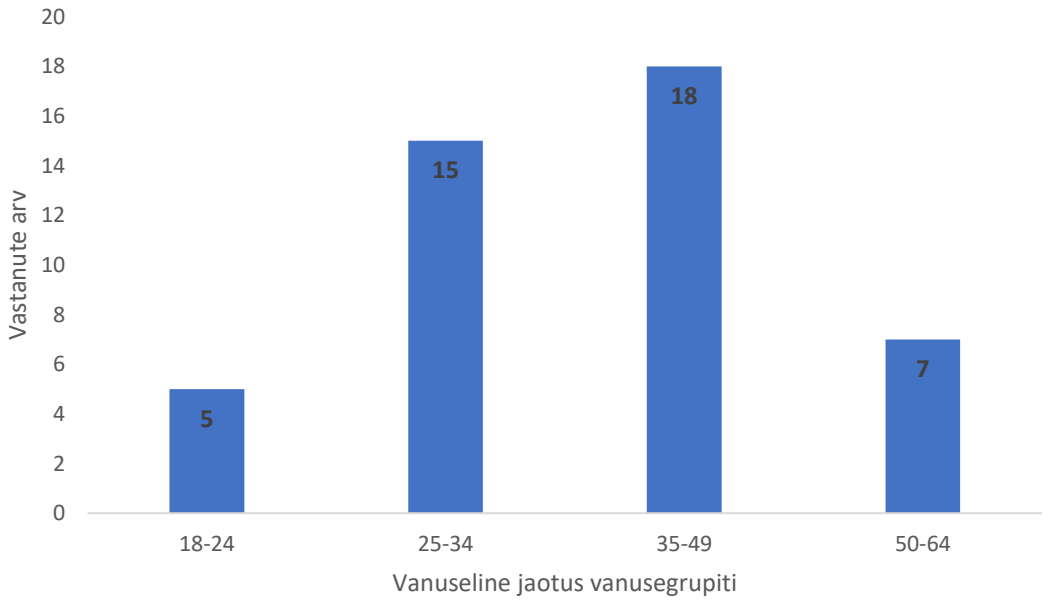
Joonisel 1 on näitlikustatud vastanute (n=45) jaotus geograafiliselt, kusjuures enim vastanuid on Võru maakonnast. See on selgitatav autoripoolse e-kirja teel edastatud ning lähimas tutvusringkonnas edastatud kutsetega uuringus osalemiseks. Teistes maakondades on vastanute jaotuse sarnane OSKA raportis kirjeldatule, kus administratiivtöötajate suurem tööhõive on Harjumaal (62%, kusjuures eraldi ei ole kajastatud Tallinna linna), Tartumaal (12,1%) ja Pärnumaal (4,2%). Vastanute hulgas ei ole Ida-Virumaal elavaid administratiivtöötajaid (kuigi ka seal on valdkonna tööhõive teistest piirkondadest suurem ehk 6,2%). Selle põhjuseks võib olla muukeelsete administratiivtöötajate suurem osakaal ning piirkonna inforuumi erinevus.



Joonis 2. Uuringus vastanute hariduslik jaotus

Vastanute hariduslikku jaotust (joonis 2) ilmestab keskerihariduse suhteliselt suurt osakaalu (31%), mis võib viidata valdkonna hääbumisele ja ka vastavalt OSKA raportile on viimase viie õppeaasta jooksul lõpetajate arv vähenenud poole võrra. Vähenemine on toimunud ühtviisi nii kutseõppes, rakenduskõrgharidus- kui bakalaureuseõppes (Kutsekoda, 2018). Samas on käesolevas uuringus osalejate hulgas 62% vastanutest kõrgharidusega. Siiski puuduvad andmed, kas tegemist on administratiivtöötaja erialale vastava kõrgharidusega või mõne muu erialaga mis annab eeldused antud erialal töötamiseks. Administratiivtöötajate amet on ka nn ohustatud ametikohtade loendis, mis tehnoloogia arengu ja digipädevuste tõusu tõttu peagi võibolla tööturult kaob. Digiturvalisuse pädevuse kontekstis peaks kõrgem haridustase looma eeldused teadlikumale käitumisele küberruumist ning kindlasti on neil töötajatel paremad IKT teadmised, kes hiljuti on õppimas käinud. See võib suurendada enesekindlust ettetulevate olukordade lahendamisel iseseisvalt hakkama saada.

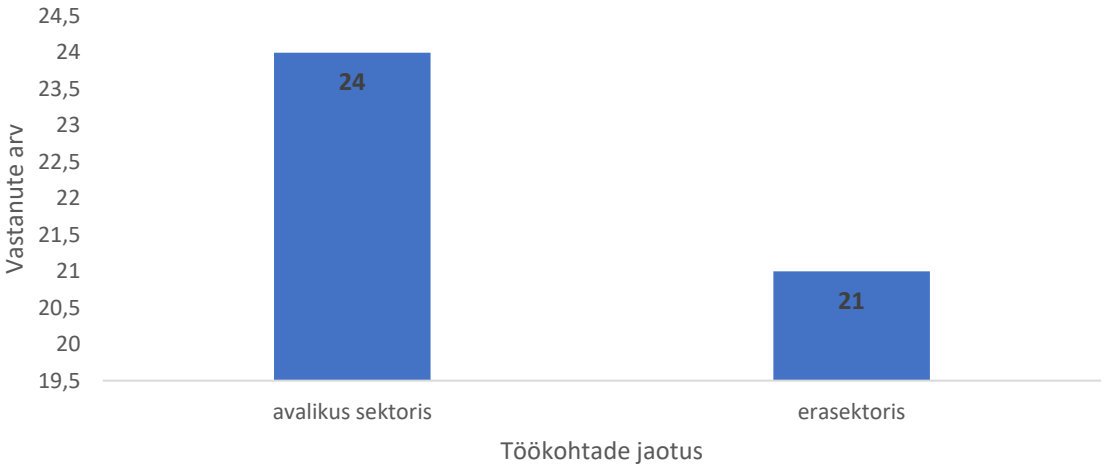
OSKA raporti kohaselt oli 2011. aastal valdkonnas 54% alla 50-aastased ja 46% üle 50-aastased. Käesolevas uuringus on vastajate vanuseline osakaal kallutatud tugevalt alla 50-aastastele. Uuringus oli kõige rohkem vastanuid vanuses 35-49 eluaastat. Kõige vähem vastanuid oli vanuses 18-24 eluaastat.



Joonis 3. Uuringus vastanute vanuseline jaotus

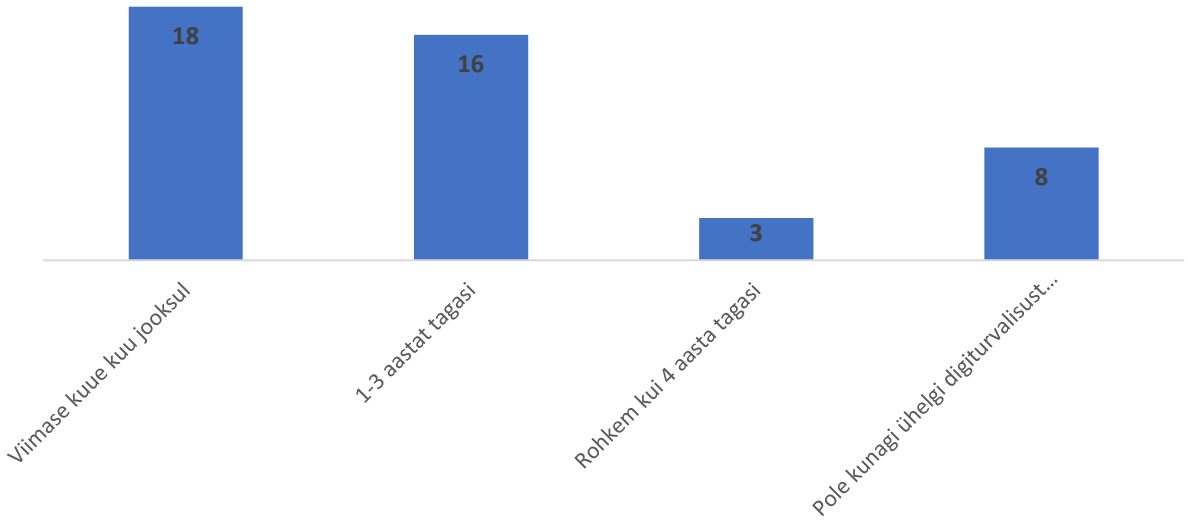
Autori hinnangul võib üheks põhjuseks olla uuringus osalemise kutse edastamise viis (sotsiaalmeedia, e-mailid), kui ka vanemaealiste üldine vähene aktiivsus uuringutes osalemiseks. Lisaks kasutas autor uuringu kutse edastamisel isikliku tutvusringkonda. Vastanute hulgas puudub oluline seos hariduse

ja vanuse vahel, st vanemaealised administratiivtöötajad ei pruugi olla kõrgemalt haritud kui nooremad (r=0,229).



Joonis 4. Uuringus vastanute töökohtade jaotus

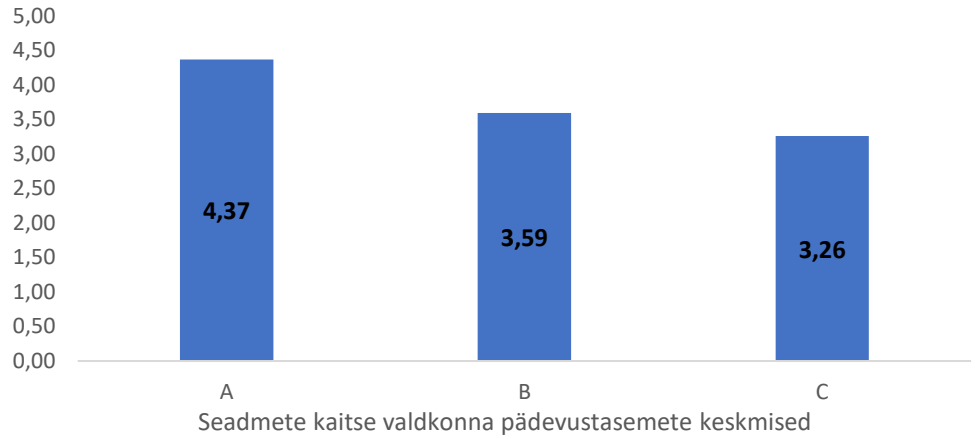
Uuringus osalejatest ~53% töötavad avalikus sektoris ja ~46% erasektoris (joonis 4). Autori hinnangul on see mõistetav, kuivõrd avalikus sektoris on administratiivtöötajate ametikohti erinevatel juhtimis- ja pädevustasanditel rohkem võrreldes erasektoriga, kus administratiivtöötajad täidavad sageli vaid sekretäri või juhiabi rolli.



Joonis 5. Uuringus vastanute digiturvalisuse koolituste läbimine

Joonisel 5 on kajastatud kas ja millal läbiti digiturvalisuse koolitusi. Tugev seos (r=0,550) esineb väite „Organisatsioon, kus töötan, on olemas digitehnoloogia turvastrateegia ja tean selle sisu“ ning digiturvalisuse pädevuse koolitusel osalemise vahel. Kuivõrd vastajad pidid väitele hinnangu andma

enne koolitusel osalemise küsimusele vastamist, võib autor hinnata, et organisatsioonid, milles turvastrateegia on kehtestatud ja jõustatud, pööravad ka rohkem tähelepanu individuaalse digiturvalisuse pädevuse arendamisele. Autori hinnangul võib seega tekkida teatav vastuolu HTM uuringuga, milles nähti organisatsioonide soovimatust oma töötajate digipädevust tõsta. Võimalik, et turvastrateegia olemasolu ei suurenda olulisel määral töötajate üldiseid digipädevusi vaid tagab läbipaistvama kontrolli ja selgemate reeglite abil organisatsiooni küberturvalisuse ning töötajatele suunatud digiturvalisuse pädevuse arengu (selgeks saavad need oskused ja teadmised, mis on turvastrateegias kehtestatud).



Joonis 6. Seademete kaitse valdkonna pädevustasemete keskmiste jaotus

Digiturvalisuse esimene valdkond on seadmete kaitse ning selle eesmärk on, et kasutajal oleks oskus kaitsta oma seadmeid ning mõista veebi riske ja ohtusid, teada ohutus- ja turvameetmeid (Ferrari, 2013).

Tabel 2. Digiturvalisuse pädevuse pädevustasemed kompetents 4.1 järgi (Ferrari, 2013)

A-algaja	B-kesktase	C-edasijõudnu
Ma oskan kasutada põhivõtteid oma seadmete kaitsmiseks (nt viirusetõrje, salasõnad jms).	Ma tean, kuidas oma digiseadmeid kaitsta ning ajakohastan oma turvastrateegiaid.	Ma ajakohastan sageli oma turvastrateegiaid. Ma oskan võtta meetmeid, kui mu seade on ohus.

Seadmete kaitse valdkonnas on enesehinnangu vastused kooskõlas pädevustasemetega. Skaalal 1-5 on keskmine 3, mis tähendab, et kõikidel juhtudel hindasid vastajad ennast üle keskmise, kuid mida kõrgem oskustase, seda madalam enesehinnang. Autori hinnangul võib seda põhjustada tõik, et

individuaalsel tasandil suudavad administratiivtöötajad seadmete kaitsmisega mehaaniliselt toime tulla, kuid mida laialdasemaks lähevad vajalikud teadmised (näiteks organisatsiooni turvastrateegia mõistmine), seda madalamaks muutub ka enesehinnang (vastavalt joonis 6 järgi A- tasemel keskmine 4,37 ja C-tasemel 3,26). SD on pädevustasemetel A=0,97; B=1,18 ja C=1,28. Kui enesehinnangu tulemused ka reaalset oskuste/teadmiste taset näitavad, siis on autori hinnangul hea, et vähemalt individuaalsetes oskustes tunnevad administratiivtöötajad ennast pigem hästi ning parandamist vajab organisatsiooni siseregulatsioonide digiturvalisuse alane ülevaatamine, kommunikeerimine ning kontroll (täidaks autori hinnangul ka õppe ja teadmiste värskenduse eesmärki).

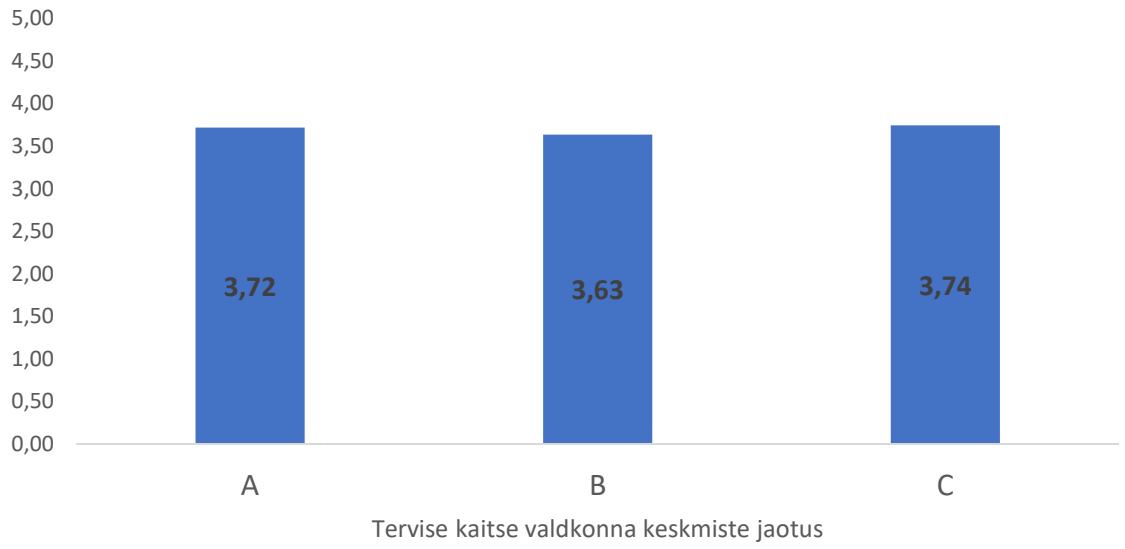
Joonis 7. Isikuandmete kaitse valdkonna pädevustasemete keskmiste jaotus

Digiturvalisuse teine valdkond on isikuandmete kaitse, mille kohaselt peaks digikasutaja mõistma ühiseid kasutustingimusi, aktiivselt kaitsma isikuandmeid, mõistma teiste inimeste õigust privaatsusele, kaitsma ennast veebipettuste ja ohtude ning küberkiusamise eest (Ferrari, 2013).

Tabel 3. Digiturvalisuse pädevuse pädevustasemed kompetents 4.2 järgi (Ferrari, 2013)

A-algaja	B-kesktase	C-edasijõudnu
Ma tean, et ma tohin enda ja teiste kohta e-keskkondades jagada ainult teatavat tüüpi infot.	Ma oskan kaitsta enda ja teiste privaatsust e-keskkonnas. Ma saan privaatsuse küsimustest üldiselt aru ja mul on põhiteadmised selle kohta, kuidas minu andmeid kogutakse ja kasutatakse.	Ma muudan sageli e-teenuste vaikesätteid, et oma privaatsuse kaitset tõhustada. Ma olen privaatsusküsimustega kursis, mul on selles valdkonnas laiad teadmised ning ma tean, kuidas minu andmeid kogutakse ja kasutatakse.

Ka selles valdkonnas on keskmised kõrgemad algaja tasemel ja madalamad kesk- ning edasijõudnute tasemel (vt joonis 7). Kuigi keskmised vastused on 1-5 skaalal üle keskmise (3), siis autori hinnangul näitab selline keskmiste jaotus seda, et päris täpselt ja detailselt isikuandmete käitlemist administratiivtöötajad siiski ei mõista. SD pädevustasemeti on A=0,78; B=0,85 ja C=1,05. Kui tavakasutaja jaoks päädib GDPR teadlikkus „küpsistega“ nõustumise või mittenõustumise dilemmadest (skaala hinne 4 „sageli“), st teadmine reeglitest on olemas, siis administratiivtöötaja peaks autori hinnangul olema teadlik tagajärgedest, mis võivad tekkida pimesi lepingute sõlmimisest (sisuliselt linnukesega kasutustingimustega nõustumisest). Seda paraku hinnati ligemale skaalapunktile 3 ehk „mõnikord“. Autori hinnangul võib see ka tähendada, et sisu kontrollitakse seal, kus see avaldab tajutavalt suuremat mõju töötajale endale. Kuigi eetiliselt peavad kõik ettevõtted käituma oma kliendi/kasutaja suhtes soosivalt, võib küberruumis leiduda ka neid, kes tahtlikult kasutajate andmeid võivad kuritarvitada.



Joonis 8. Tervise kaitse valdkonna pädevustasemete keskmiste jaotus

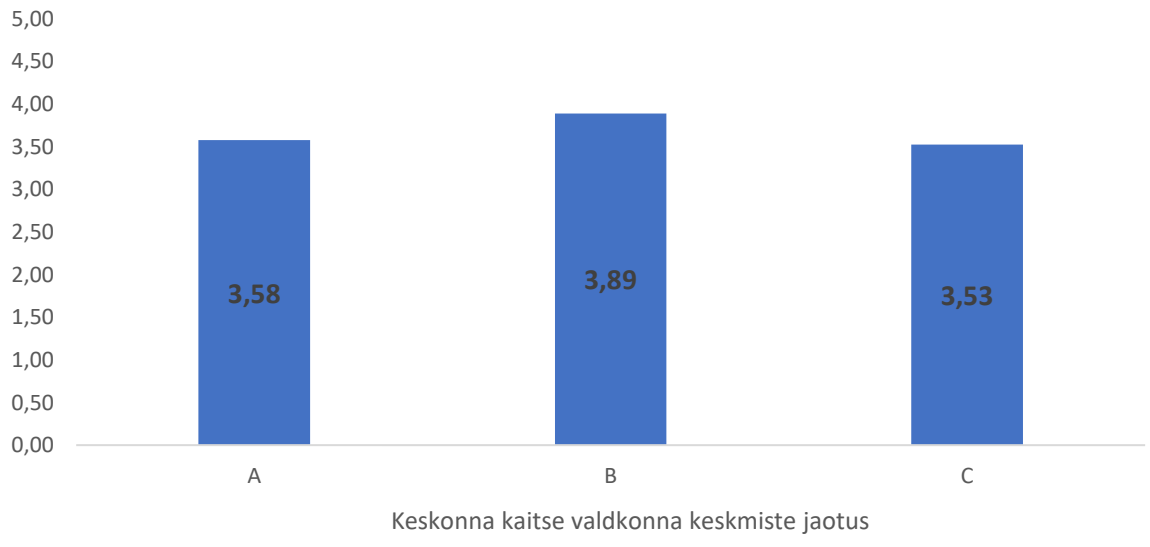
Digiturvalisuse kolmas valdkond on tervise kaitse ning selle eesmärk on vältida tehnoloogiliste vahendite kasutamisega seotud terviseriske, sh ohtu füüsilisele ja vaimsele heaolule (Ferrari, 2013).

Tabel 4. Digiturvalisuse pädevuse pädevustasemed kompetents 4.3 järgi (Ferrari, 2013)

A-algaja	B-kesktase	C-edasijõudnu
Ma tean, kuidas vältida küberkiusamist. Ma tean, et tehnoloogiliste vahendite	Ma tean, kuidas kaitsta ennast ja teisi küberkiusamise eest ning mõistan tehnoloogiliste vahendite kasutamisega seotud	Ma tean, kuidas kasutada tehnoloogilisi vahendeid nii, et vältida terviseprobleeme. Ma tean, kuidas leida hea tasakaal

väärkasutus võib kahjustada minu tervist.	terviseriske (alates ergonoomika aspektidest kuni tehnoloogiasõltuvuseni).	e-maailma ja füüsilise maailma vahel.

Et vastuste keskmine jääb läbivalt kõrgemaks kui skaala keskmise (3) ja pädevustasemete vahel märkimisväärseid keskmiste erinevusi ei ole (vahe maksimaalselt 0,11 punkti), seega järeldab autor, et administratiivtöötajad võivad enesehinnanguna tunda, et tervise teematika on oluline, kuid kindlust digitaalse enesekaitse kontekstis ei ole. Siiski on hinnangud lähemal skaalapunktile 4 ehk „sageli“, millest võiks järeldada, et administratiivtöötajad oskavad oma tervist hoida. SD pädevustasemeti on A=1,06; B=1,10 ja C=0,86. Kuivõrd pauside olulisusest on räägitud meedias (MTÜ Peaasi) ja kuvariga töötajatele isegi kehtestatud terviskaitset reguleeriv määrus (kuvariga töötamise töötervishoiu ja tööohutuse nõuded), siis praktilised oskused digitöörütmi reguleerimiseks võivad olla puudulikud. Autori hinnangul vajab selliste oskuste juurutamine kaasaegset töökeskkonda ja organisatsiooni töötajasõbralikku kultuuri, st ruum ja inimesed peavad soodustama ja toetama töökohal tervisele tähelepanu juhtimist. Samas võib käesoleva uurimuse raames olla keskmiste võrdne jaotus tingitud ka pädevustasemete väidete sarnasest sõnastusest, ent isegi siis hindavad administratiivtöötajad oma oskusi-teadmisi tervise valdkonnas nii algaja ja edasijõudnu tasandil madalamalt. Siinkohal on tähtsal kohal töötervishoiu eest vastutava töötaja olemasolu ning töö eesmärgistatus.



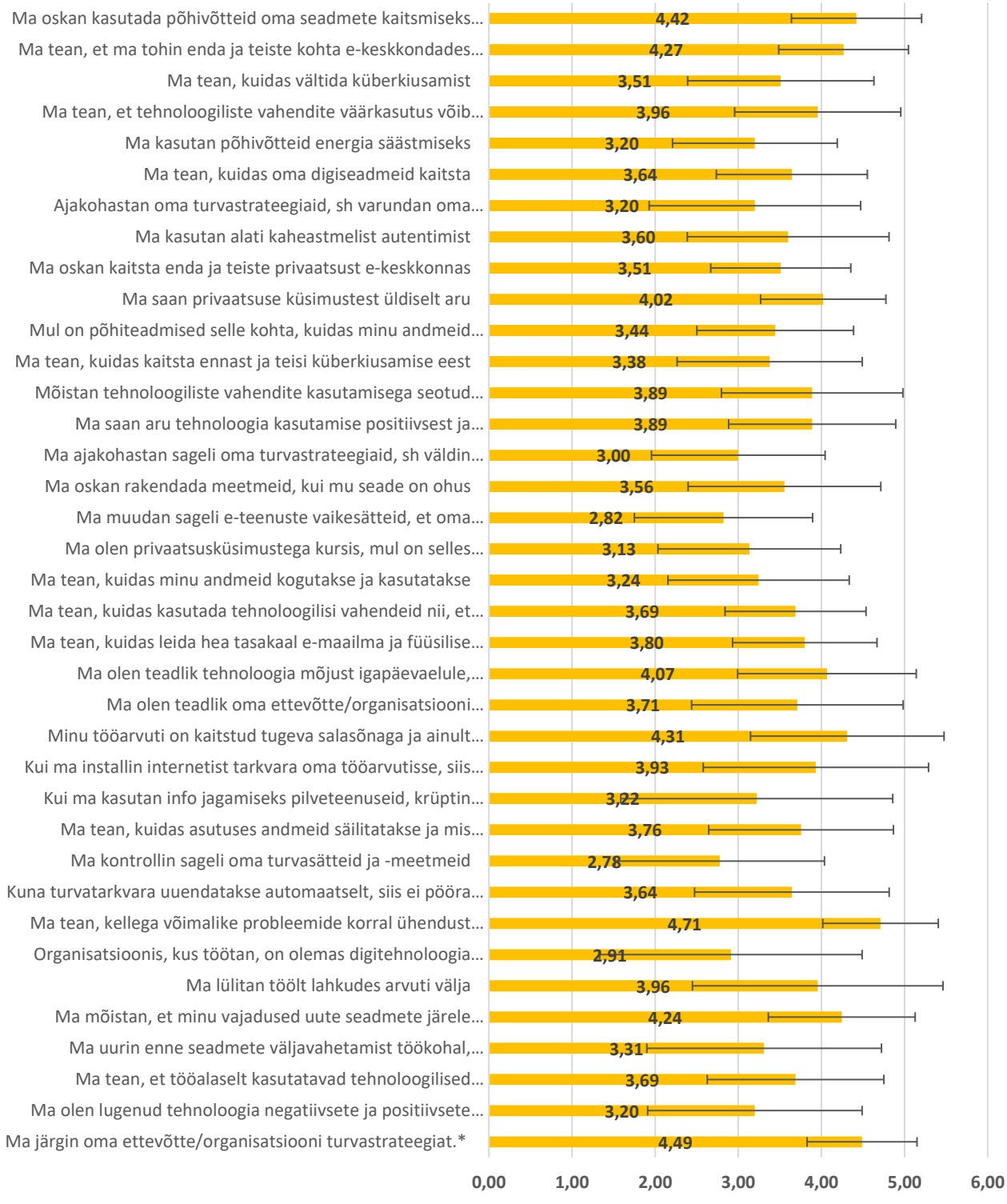
Joonis 9. Keskkonna kaitse valdkonna pädevustasemete keskmiste jaotus

Digiturvalisuse neljas valdkond on keskkonna kaitse ning selle eesmärk, et kasutaja oleks teadlik IKT mõjust keskkonnale (Ferrari, 2013).

Tabel 5. Digiturvalisuse pädevuse pädevustasemed kompetents 4.4 järgi (Ferrari, 2013)

A-algaja	B-kesktase	C-edasijõudnu
Ma kasutan põhivõtteid energia säästmiseks.	Ma saan aru tehnoloogia kasutamise positiivsest ja negatiivsest mõjust keskkonnale.	Ma olen teadlik tehnoloogia mõjust igapäevaelule, veebitarbimisele ja keskkonnale.

Administratiivtöötajate hinnangud keskkonnakaitse valdkonnale digiturvalisuse pädevuses ületasid jällegi skaala keskmist (3), olid suhteliselt väikese erinevusega (max 0,36 punkti), kuid lähemal hindele 4 ehk „sageli“ olid vastused B-taseme väitele. SD pädevustasemeti on A=1,25; B=1,01 ja C=1,26. Autori hinnangul võib see viidata, et kuigi positiivset ja negatiivset mõju keskkonnale tajutakse, ei väljendu see alati tegevustes. Nii näiteks võib arvutiga töötamisel taustal mängida hoopis televiisor, mis siis „tühjalt“ energiat sööb. Samas võib A-taseme hinnangud madalamaks viia avalikus sektori levinud keskne tarkvarauuenduste läbiviimise meetod, kus väljaspool tööaega peavad seadmed olema võrgus ja sisse lülitatud (st sisekorraldusega on keelatud seadmete väljalülitamine). Autori hinnangul võib taseme C suhteliselt madalam hinnang olla seotud põhimõttega, et keskkonnakaitsest kontseptuaalselt saavad administratiivtöötajad aru, kuid kehvem on seis detailide vaates, ehk praktilisi keskkonnahoiu tegevusi ilmselt teadlikult ei tehta.



Joonis 10. DigComp enesehinnangu väidete keskmine ja standardhälve

„Ma järgin oma ettevõtte/organisatsiooni turvastrateegiat“ on standardhälve (SD) 0,66 (näitab keskmist erinevust keskmisest) ja keskmine hinne 4,49 (kõrge), millest võib järeldada, et vastanud järgivad ettevõtte/organisatsiooni turvastrateegiaid ning on andnud sellele digiturvalisuse pädevusel kõrgemad hinded. Väide „Ajakohastan oma turvastrateegiaid, sh varundan oma tööfaile“ SD on

kõrge=1,27 ning keskmine madal= 3,20, mis näitab, et vastuste hajuvus ümber keskmise on suurem. Vastanute seas on enesehinnanguna antud väite kohta hinnatud tegevust maksimaalse tulemusega ning samas on vastajaid, kes hindasid väidet madalamalt. Siin võib olla põhjuseks olukord, kus tööfailide varundamine on antud ettevõttes/organisatsioonis määratud konkreetsete spetsialistide töökohustusteks ning administratiivtöötaja ei tee seda ise või ei tea, et seda tehakse tema eest.

Esinevad seosed läbitud digiturvalisuse pädevuse koolituse ja järgnevate enesehinnangu väidete vahel:

1. „Organisatsioonis, kus töötan, on olemas turvastrateegia“ väitega on tugev oluline seos (r=0,550);
2. „Ma oskan rakendada meetmeid, kui mu seade on ohus“ väitega on tugev oluline seos (r=0,510);
3. „Ma oskan kaitsta enda ja teiste privaatsust e-keskkonnas“ väitega on tugev oluline seos (r=0,578);
4. „Ma tean, kuidas oma digiseadmeid kaitsta“ väitega on tugev oluline seos (r=0,516).
5. Kokku esineb 36st väitest üle keskmise tugevusega (r>0,3) seos koolitusega 21 juhul, mis näitab spetsiifiliste digiturvalisusega seotud koolituste olulisust enesehinnangu kujundamisel. Autori hinnangul peaksid seega organisatsioonid süstemaatiliselt tegelema digiturvalisuse alase koolitustegevusega.

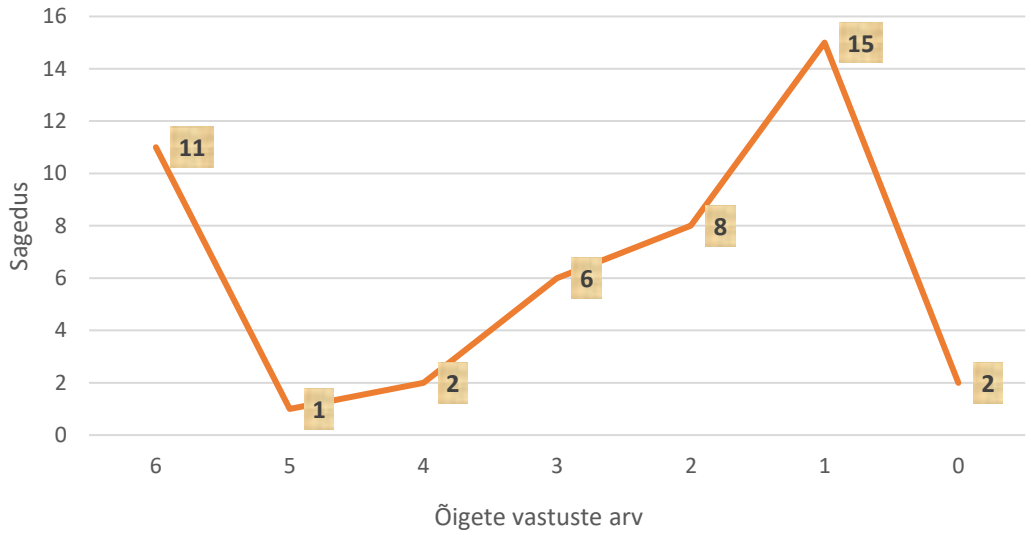
Seose tugevus on oluline lisaks koolitusele endale ka viimase koolituse toimumise aja suhtes, st mida värskemad on omandatud teadmised ja oskused, seda kõrgem on vastanute enesehinnang. Autori hinnangul annab eelnev kinnitust, et digiturvalisuse pädevuse omandamiseks on parim viis selgus organisatsiooni turvastrateegias (et töötajad oskaksid vastavalt reeglitele käituda) ning et digiturvalisuse alased koolitused peaksid olema integreeritud organisatsiooni kultuuri sisse vähemalt iga-aastase täiendõppena.

Esineb keskmine seos haridustaseme ja väite „Ma uurin enne seadmete väljavahetamist, millised on parimad saadaolevad …“ (r=0,426). Autor hinnangul võib see viidata kõrgema haridustasemega administratiivtöötajate juhtivamale töörollile, kus valikuvabadus- ja kohustus seadmete valikul on suurem ning finantsvahendid juhtivtöötaja enda hallata.

Lisaks esineb keskmine seos haridustaseme ja järgmiste väidete vahel:

1. „Minu tööarvuti on kaitstud tugeva parooliga“ (r=0,362);
2. „Ma tean, kuidas … kasutada tehnoloogiat … vältida terviseprobleeme“ (r=0,317).

Autori hinnangul võib see tähendada, et administratiivtöötaja, kes on kõrgemalt haritud, on lihtsalt rohkem kokku puutunud digiturvalisuse temaatikaga. Kuigi autor ei ole uurinud hariduse tunnuse ajalist väärtust (kes millal viimase tasemeõppe lõpetas) võib siiski eeldada, et kaasaegses tasemeõppes käsitletakse vähemalt mingis ulatuses digiturvalisuse teemat. Samuti on kasutajate paroolituralisuse teadlikkusele kaasa aitamas ka veebiettevõtjad ise, juhendades kasutajaid nt parooli turvalisuses veenduma. Autori hinnangul hakati tehnoloogia ja terviseprobleemide seosele suuremat tähelepanu pöörama just COVID-19 tingitud kaugtöö mahu suurenemise tõttu ja ka kontoritööga seotud suurendatud tähelepanust läbipõlemisele. Eriti hoolikalt käsitletakse selliseid teemasid kõrgharidusõppes.



Joonis 11. Situatsioonülesande 1 õigete vastuste sagedus

Joonisel 11 on kujutatud situatsioonülesande 1 õigete vastuste sagedused. Vastanutest 30% määrasid neli või enamat parooli õigesti.

Vastajate vanuse ja situatsioonülesanne 1 vahel esineb keskmise tugevusega negatiivne seos (r=-0,342). Autori hinnangul on vastanute vanus pöördvõrdelises seoses nende õigete vastuste arvuga. See võib viidata, et nooremad vastajad mõistavad parooli koostamise loogikat, samas kui vanemad vastajad on harjunud mehaaniliselt täitma organisatsiooni turvastrateegiat.

Situatsioonülesande 2 puhul ei esinenud seost tervise ja keskkonna ohuteguritega. Kuna antud valimiga olulisi seoseid ei esine, siis on autoril võimatu anda hinnangut situatsioonülesande 2 digiturvalisuse pädevuse hindamiseks.

Esineb keskmise tugevusega negatiivne seos situatsioonülesande 3 ja järgnevate väidete vahel:

1. „Ma tean, kuidas asutuses andmeid säilitatakse ja mis privaatsus….“ (r=-0,338);
2. „Ma olen teadlik on organisatsiooni turvastrateegiast“ (r=-0,338).

Autori hinnangul võib selline seos viidata organisatsiooni turvastrateegia selgusele ja vastajate teadlikkusele, et IKT eeskirjade rikkumise eest võib järgneda sanktsioon. Meelelahutusportaalide puhul ei pöörata aga sageli tähelepanu kasutuslepingute sisule, kuivõrd vastajad võivad hinnata, et tegemist on privaatsusreegleid mitterikkuvate keskkondadega. Autori hinnangul ei tohiks veebikeskkondade kasutuslepingud olla kasutajatele lugemiseks keerukad ja mahukad – tähelepanu peab olema juhitud olulistele tehnilistele nüanssidele (nt mõistlike ettevõtete küpsiste seadete puhul) ja mitte püüdele matta kasutajaid segadusttekitavasse bürokraatiasse.

Muude tabelis 1 kajastatud digipädevuste ja situatsioonülesande 3 vahel seosed puuduvad või on nõrgad. Autori hinnangul viitab see käesoleva lõputöö raames sellele, et ülesande lahenduses teadmised meelelahutuskeskkondade kasutuslepingu sisust on puudulikud, kuivõrd sealsetele tehnilistele nüanssidele ei osata ka tähelepanu pöörata. Järelikult on küsimus vastajatele uudne ning keskkondade privaatsussätetele ei ole varasemalt mõeldud. Autori hinnangul võiks sellist situatsioonülesannet korrata töökeskkonnas kasutusel oleva tarkvara privaatsuslepinguga või kavandada situatsioonülesanne tegeliku kasutustingimustega nõustumise ülesandega, et mõõta, kui paljud kasutajad lepingu avavad või selle lõpuni loevad ja hiljem, kuidas nad seal leidunud „konksudest“ aru said.

Situatsioonülesande 4 puhul vastas 25 uuringus osalejat küsimusele õigesti („Otsin abi“) ja 20 valesti („Avan kahtlase faili“ või „Vajutan allalaadimise aknale“). Situatsioonülesanne oli üles ehitatud selliselt, et õige vastus eeldanuks enesekontrolli „minnalaskmist“, kuid digipädevuse kasvades on autori hinnangul oht, et enda võimeid hinnatakse üle. Koostatud situatsioonülesanne võib autori hinnangul olla kallutatud, kuna ei arvesta erinevate veebilehitsejate ja operatsioonisüsteemide eripäradega. Niisamuti katkestaks autori hinnangul kasutajad ebaturvalise käitumise varem, kui käesolev situatsioonülesanne seda võimaldas. Siiski leiab autor, et ülesande lahendamine nõudis süvenemist ja enesekontrolli. Esinevad olulised seosed situatsioonülesande 4 ja järgnevate väidete vahel:

1. „Ma tean kuidas oma digiseadmeid kaitsta“ (r=-0,503)
2. „Ma oskan rakendada meetmeid kui mu seade on ohus“ (r=-0,386)
3. „Ma tean kuidas asutuses andmeid säilitatakse ja mis privaatsuspõhimõtteid rakendatakse“ (r=-0,443)
4. „Kui ma installin internetist tarkvara tööarvutisse…kontrollib faili ennem allalaadimist“ (r=-0,378)

Autori hinnangul on võib siin negatiivne korrelatsioon olla seotud digipädevuse kõrge hinnanguga seotud liigse enesekindlusega – st vastajad tajusid enda kontrolli olukorra üle suuremana, kui see tegelikult oli. Lisaks on viiteid õpitud abitusele, kus tarkvarakontrolli tarkvara ja asutuse turvastrateegia selgus võivad kasutajad muuta mugavaks ning loovutada inimliku kontrolli tehnilisele kontrollile.

3.5 Järeldused

Situatsiooniülesanded nr 1, 3 ja 4 esitasid väljakutse enesehindamisküsimustikule. See tähendab, et nende situatsioonülesannetega oli võimalik (ülesehitusest tingitud piirangutega arvestades) kontrollida enesehinnangu vastavust tegelikele digipädevustele. Situatsioonharjutuse nr 2 puhul käesoleva lõputöö raames seoseid ei esinenud, mistõttu on autoril testi toimivusele keeruline hinnangut anda.

Enesehinnang oli seda kõrgem, mida hilisemalt oli läbitud digiturvalisuse alane koolitus või infopäev ja seda kõrgem oli ka tajutud teadlikkus organisatsiooni turvastrateegiatest. Sellest võib järeldada, et digiturvalisuse pädevus administratiivtöötajate seas on lihtsamini omandatav siis, kui organisatsioon koolitab oma inimesi süsteemselt ning digiturvalisuse reeglistik on läbipaistev, arusaadav ning kõigile kättesaadav ja teadvustatud.

Uuringu piirangud:

- Küsimustik võimaldas situatsiooniülesannete järgselt tagasiliikumist enesehinnangu küsimusteni. Kui situatsioonülesanne tundus liiga raske kuid enesehinnangu küsimuses algselt hinnati ennast reitinguskaalal „5“ või „4“ siis võis vastaja seda muuta reitinguskaalal väiksema väärtusega tulemuseks nii, et seos hinnangu ja situatsioonülesande vahel muutus.
- Situatsioonülesande 1 puhul võis uuringu tulemusi mõjutada pildi kvaliteet ning vastajad ei saanud aru ülesande detailidest.
- Liiga väike vastanute hulk ei võimalda teha usaldusväärseid järeldusi kogu populatsiooni kohta.

Soovitused edasiseks uurimiseks

- Situatsioonülesannete väljatöötamine vajab tarkvarapõhisust. Näiteks on veebilehitsejate Google Chrome ja Safari allalaadimise liidesed erineva väljanägemise ja käskluste korraldustega, niisamuti võivad sageli operatsioonisüsteemi pahavaratõrje tarkvarad käivituda või lukustada arvuti enne pahavara avamist.

- Kohandada situatsioonülesanded ja enesehinnangu küsimustiku sõnastust selgemaks ja oskuste tasemete kaupa eristuvamaks ning viia uuring läbi suurema valimi peal.
- 2022. aasta märtsis uuendati DigCompi mudelit (DigComp 2.2), mistõttu käesoleva lõputöö enesehindamisküsimustik tuleb korrigeerida täiendatud mudelile vastavaks.

KOKKUVÕTE

Administratiivtöö on järjest enam liikumas digiruumi ja üha rohkem nõutakse administratiivtöötajatelt digiturvalisuse valdkonnas heade pädevuste omamist. Selle tõttu püstitas autor lõputöö eesmärgi, et sõnastada DigComp mudeli abil administratiivtöötajatele sobivad väited enesehindamisküsimustiku jaoks digiturvalisuse pädevuse valdkonnas ja testida enesehinnanguid situatsioonülesannetega.

Digipädevused DigComp mudelis on jaotatud viide suurde kategooriasse: info ja andmekirja oskus, suhtlus ja koostöö digikeskkonnas, digisisu loomine, digiturvalisus ja probleemilahendusoskus. Käesolevas lõputöös kasutas autor teadlikult vaid digiturvalisuse küsimusi, kuid ka teised digipädevused panustavad ülekantavalt digiturvalisuse valdkonda.

Lõputöö raames kasutati digiturvalisuse pädevuse mõistet järgnevalt: digiturvalisuse pädevus tähendab inimese käitumist küberruumis ja IKT seadme kasutamisel selliselt, et ta ei sea ohtu privaatelu turvalisust, organisatsiooni turvalisust, inimese tervist ega teda ümbritsevat keskkonda. Lisaks digiturvalisuse mõistele on lõputöös kasutatud ka mõisteid küberhügieen (digihügieen), küberturvalisus ja infoturvalisus ning selgitatud nende sidusust digiturvalisuse pädevusega. Lõputöö tugineb 2013. aastal koostatud Euroopa Komisjoni digipädevuse raamistikule DigComp, milles on kirjeldatud igalt Euroopa Liidu kodanikult oodatavad digitaalsed oskused, teadmised ja hoiakud ning mille najalt on nii Eestis kui mujal maailmas süstematiseeritud digipädevuste arendamist eeskätt õpetajate ja õpilaste vaates. Et sarnaseid põhimõtteid laiendada erialaspetsiifiliselt, kitsendas autor oma uurimisvaldkonda administratiivtöötajatele, keda Eestis 2013. aasta OSKA raporti järgi on ca 22 000. Lõputöö andmed kogus autor veebiküsitluse abil ning kutse uuringus osalemiseks saadeti e-maili ja sotsiaalmeedia vahendusel, kuid valimi suurus (n=45) ei ole esinduslik kogu populatsioonile (95% usaldusnivooga ja 10% usaldusvahemikuga olnuks see 96), kuid enesehindamisküsimustiku asjakohasuse kohta sai autor siiski järeldusi teha. Autor kasutas tulemuse analüüsimiseks kirjeldavat statistikat, Spearmani seosekordajat enesehindamise väidete, demograafiliste näitajate ja situatsioonülesannete vastuste vahel, digiturvalisuse pädevuse kompetenteside enesehinnangute keskmiste võrdlust ja standardhälbeid.

Enesehindamisküsimustiku vastuste analüüsimisel selgus, et organisatsioonide ja koolituste roll administratiivtöötajate enesehinnangule on suur – mida hiljem on läbitud digiturvalisuse alane täiendkoolitus vms, seda kõrgemalt hindasid uuringus osalejad oma digipädevusi. Sarnast efekti omas ka organisatsiooni turvastrateegia rolli mõistmine.

Eneesehindamisküsimustiku ja situatsiooniülesannete võrdluses leidis kinnitust asjaolu, et kõrge enesehinnang võib vastajates tekitada liigset enesekindlust, mistõttu võib võimenduda iseteadlikkusest tingitud riskikäitumine ning vähene suutlikkus abi otsida näiteks IT spetsialistilt.

Kuivõrd 2022. aastal koostati täiendatud DigCOMP 2.2 mudel, siis võimaldaks see digipädevuste hindamist veel paremini, ent eneseanalüüsist ainukesena ei piisa. Autori seisukoht on, et situatsioonülesannete lahendamine aitab pöörata tähelepanu valdkondadele, milles administratiivtöötajad eriliselt tähelepanelikud peavad olema. Näiteks digiruumi kasutuslepingute sisu mõistmine, et vältida sensitiivse informatsiooni kättesaadavaks tegemist, sh näiteks pilveteenuste puhul. Võtmetähtsusega on digiturvalisuse pädevuste arendamise süsteemsus ja samas muutlikkus, et kujundada administratiivtöötajates harjumus järjest suureneva digitööga tervisele ja keskkonnale ohutult toime tulla. Selleks vajab aga muutumist ka organisatsioonide töökultuur ja vaated digiturvalisuse valdkonnale.

SUMMARY

Administrative personnel are more and more inclined towards digital work and thus are expected to have a higher proficiency level also in the field of digital security. For this particular reason, the purpose of this final thesis was to develop a suitable questionnaire for self-evaluation of administrative personnel and test the respondent's self-evaluation with situational tasks in order to identify, whether theory is being put into practice.

The author based the study on European Commission Digital Competency Framework from 2013 (DigCOMP), which defines five categories for digital competencies. These include digital literacy, communication and cooperation, creation of digital content, digital security and troubleshooting.

In this final thesis, the author deliberately used only knowledge, skills and attitudes of the digital security competency, although all the other digital competencies also contribute to the security field as well.

The author uses digital security competency term as follows: actions of a person in cyberspace and while using information- and communication technology devices in a way, that does not create harm to the person, the environment, the person's private life and also the organisational security.

The studies conducted in the digital security field have been contributing to student and teacher competencies. In order to apply the aspects of research to administrative personnel, the author asked workers in the field to reply to an electronic questionnaire. The sample size was small (n=45) and thus the results of this research paper are not applicable to the whole population of Estonian administrative workers (n=22000), but questions regarding the suitability of the self-evaluation questionnaire could be answered and tested with situational tasks. The key results of this final thesis are, that in order to develop digital security competencies, there is relevance in the time lapsed between the last training and answering the questionnaire. This puts an emphasis on how organizations should systematically deal with training their own personnel in the ways of digital security. The testing with situational tasks also revealed, that there is possibility for self-evaluated overcompensation in tasks, which require seeking for help from other parties due to the perceived independence and self-control. Due to the fact, that in 2022 a new version of DigCOMP 2.2 model was created, this study should be repeated on a bigger sample and emphasis put on the creation of system specific situational tasks.

VIIDATUD ALLIKAD

[ITS] IT terministandardi sõnastik. (*s.a.*). Kasutamise kuupäev: 25.03.2022, allikas http://www.eki.ee/dict/its/index.cgi?Q=infoturve&F=M&C06=et&C10=1

Awareness of the DigComp framework among the CEPIS community. (*s.a.*). Kasutamise kuupäev: 23.03.2022, allikas www.cepis.org: https://cepis.org/digcomp-report-2021/

L. Birgy, T. Sõmer, K. Osula, K. Ääsmäe & M.-L. Üürike. (2018). *KüberPähkli uuring*. Kasutamise kuupäev: 26.04.2022, allikas https://docs.google.com/document/d/1SpZR_a4hNITSA0M8TqPS0LCcWro8ZOYECGBypgn91OI/edit#heading=h.gjdgxs

B. S. Bloom, M. D. Engelhart, E. J. Furst, H. Walker & D. R. Krathwohl. (1956). *Taxonomy of educational objective.* Kasutamise kuupäev: 02.04.2022, allikas https://web.archive.org/web/20201212072520id_/https://www.uky.edu/~rsand1/china2018/texts/Bloom%20et%20al%20-Taxonomy%20of%20Educational%20Objectives.pdf

Digipädevus maailmas. (*s.a.*). Kasutamise kuupäev: 09.04.2022, allikas https://digipadevus.ee/digipadevus-maailmas/

Eesti digiühiskond 2030. (2021). Kasutamise kuupäev: 25.03.2022, allikas https://mkm.ee/sites/default/files/mkm_arengukava_digiuhiskond_26-10-2021.pdf

e-governance. (*s.a.*). Kasutamise kuupäev: 13.06.2022, allikas e-estonia: https://e-estonia.com/solutions/e-governance/

Ettevõtte küberturvalisuse lühijuhend. (2019). Kasutamise kuupäev: 25.03.2022, allikas https://www.ria.ee/sites/default/files/lisa_5._ettevotte_kyberturvalisuse_lyhijuhend_eesti_keeles.pdf

Euroopa Komisjon. (2021). *The Digital Economy and Society Index — Countries' performance in digitisation.* Kasutamise kuupäev: 24.04.2022, allikas Euroopa Komisjon: https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

A. Ferrari. (2013). *DIGCOMP: Kuidas arendada ja mõista digipädevust Euroopas?* Kasutamise kuupäev: 18.06.2022, allikas: https://www.hm.ee/sites/default/files/digipadevuse_enesehindamise_raamistik_0.pdf

Haridusvaldkonna arengukava 2021-2035. (*s.a.*). Kasutamise kuupäev: 26.03.2022, allikas https://www.hm.ee/sites/default/files/eesti_haridusvaldkonna_arengukava_2035_seisuga_2020.03.27.pdf

M. Himma. (2018). *Teadlane teab, mis on küberturvalisus*. Kasutamise kuupäev: 25.03.2022, allikas https://novaator.err.ee/687133/teadlane-teab-mis-on-kuberturvalisus

Infotöötlusoskused ja näidisülesanded. (2021). Kasutamise kuupäev: 25.03.2022, allikas https://www.hm.ee/et/naidisulesanded

Kaitseministeerium. (*s.a.*). *Eesti julgeolekupoliitika alused.* Allikas: www.kaitseministeerium.ee: https://kaitseministeerium.ee/sites/default/files/sisulehed/eesmargid_tegevused/395xiii_rk_o_lisa.pdf?fbclid=IwAR1w9Wu1gYh_gDgwraRBKwIqfCvXaV5rKOm0nEaoxepG18FSGT_VAZgeHuE

Kutsekoda. (2018). *Tulevikuvaade tööjõu- ja oskuste vajadusele.* Kasutamise kuupäev: 10.04.2022, allikas https://oska.kutsekoda.ee/wp-content/uploads/2018/06/Personali-administratiivt%C3%B6%C3%B6-ja-%C3%A4rin%C3%B5ustamise-uuring.pdf

Kutsekoda. *OSKA ülevaade valdkonnaspetsiifiliste IKT-oskuste vajadusest.* (2020). Kasutamise kuupäev: 23. 04.2022, allikas https://oska.kutsekoda.ee/wp-content/uploads/2020/06/OSKA-%C3%BClevaade-valdkonnaspetsiifiliste-IKT-oskuste-vajadusest_16.06.2020.pdf

Kutsestandardid: Sekretär, tase 5. (*s.a.*). Kasutamise kuupäev: 25.03.2022, allikas https://www.kutseregister.ee/ctrl/et/Standardid/vaata/10643943

Küberkuriteod. (*s.a.*). Kasutamise kuupäev: 14.04.2022, allikas: https://www.kriminaalpoliitika.ee/kuritegevus2020/kuberkuriteod/?fbclid=IwAR2Z4XpZdlxjpi1SSGYc14JoE6IjhMPEyvtlHNVdv-Cbo3iWO3F-k3ASMXo

Naiskodukaitse. (*s.a.*). *OLE VALMIS!* Kasutamise kuupäev: 14.06.2021, allikas www.naiskodukaitse.ee: https://www.naiskodukaitse.ee/OLE_VALMIS_3680

OECD. (*s.a.*). *Digital security*. Kasutamise kuupäev: 24.03.2022, allikas https://www.oecd.org/sti/ieconomy/digital-security/

J. Palm. (2021). *Küberruumis olgu aknad ja uksed suletud*. Kasutamise kuupäev: 29.03.2022. a., allikas https://www.sekretar.ee/uudised/2021/01/18/kuberruumis-olgu-aknad-ja-uksed-suletud

V. Parve. (2021). *Lollikindlat IT-süsteemi pole olemas ja seetõttu tuleb hoida ettevõtte IT terava pilgu all.* Kasutamise kuupäev: 25.03.2022, allikas https://www.aripaev.ee/sisuturundus/2021/06/11/lollikindlat-it-susteemi-pole-olemas-ja-seetottu-tuleb-hoida-ettevotte-it-terava-pilgu-all

Rahvusvaheline täiskasvanute oskuste uuring PIAAC. (*s.a.*). Kasutamise kuupäev: 13.02.2022, allikas www.hm.ee: https://www.hm.ee/et/tegevused/uuringud-ja-statistika/rahvusvaheline-taiskasvanute-oskuste-uuring-piaac

Riigi Infosüsteemi Amet. (2022). *Trendid ja tähelepanekud küberruumis – I kvartal 2022*. Kasutamise kuupäev: 09.04.2022, allikas https://www.ria.ee/et/uudised/trendid-ja-tahelepanekud-kuberruumis-i-kvartal-2022.html

K. Rootalu. (2014). *Sotsiaalse analüüsi meetodite ja metoloogia õpibaas*. Kasutamise kuupäev: 13.03.2022, allikas www.ut.ee: https://samm.ut.ee/korrelatsioonikordajad

Set up iCloud Keychain. (2022). Kasutamise kuupäev: 20.04.2022, allikas https://support.apple.com/: https://support.apple.com/en-us/HT204085

T. Sõmer, B. Lorenz, S. Mäses & T. Muulmann. *(s.a.). Küberkaitse*. Kasutamise kuupäev: 27.03.2022, allikas https://web.htk.tlu.ee/digitaru/kyberkaitse/chapter/seadused-ja-regulatsioonid

Sõnastik. *(s.a.*). Kasutamise kuupäev: 23.03.2022, allikas www.digipadevus.ee: https://digipadevus.ee/sonastik/digiturvalisus/

Sõnaveeb. *(s.a.*). Kasutamise kuupäev: 10.04.2022, allikas https://sonaveeb.ee/search/unif/dlall/dsall/k%C3%BCberh%C3%BCgieen/1

Tartu Ülikool. *(s.a.*). *Digipädevuse enesetest*. Kasutamise kuupäev: 10.04.2022, allikas: https://sisu.ut.ee/digipadevus/quiz/enesetest

The Digital Economy and Society Index (DESI). (*s.a.*). Kasutamise kuupäev: 26.04.2022, allikas https://digital-strategy.ec.europa.eu/en/policies/desi

Tööandjad saavad uuest aastast toetust töötajate digioskuste arendamiseks. (2020). Kasutamise kuupäev: 22.04.2022, allikas https://raha.geenius.ee/blogi/tootukassa-blogi/tooandjad-saavad-uuest-aastast-toetust-tootajate-digioskuste-arendamiseks/

R. Vuorikari, S. Kluzer & Y. Punie. (2022). *Digital Competences Framework (DigComp 2.2) update published.* Kasutamise kuupäev: 23.04.2022, allikas: https://ec.europa.eu/social/main.jsp?langId=en&catId=89&newsId=10193&furtherNews=ye

L. Õunapuu. (2014). *Kvalitatiivne ja kvantitatiivne uurimisviis sotsiaalteadustes.* Tartu Ülikool. Kasutamise kuupäev: 10.04.2022, allikas http://dspace.ut.ee/bitstream/handle/10062/36419/ounapuu_kvalitatiivne.pdf

A. Ääremaa, (*s.a.*). *Digipöörde programm 2019-2022.* Kasutamise kuupäev: 12.04.2022, allikas: https://www.hm.ee/sites/default/files/2_digiprogr_2019_22_seletuskiri_28dets18.pdf

LISAD

Lisa 1. Küsimustik administratiivtöötajate digiturvalisuse pädevuse kaardistamiseks

Lisa 2. Situatsioonülesanded

Lisa 3. Eesti õppijate digipädevusmudeli digiturvalisuse komponendi ja DigComp digiturvalisuse väidete võrdlus

Lisa 4. Korrelatsioonimaatriks

Lisa 1. Küsimustik administratiivtöötajate digiturvalisuse pädevuse kaardistamiseks

Tere!

Olen Tallinna Tehnikakõrgkooli III kursuse teabehalduse ja infosüsteemide korraldamise eriala tudeng. Palun Teie abi uuringu läbiviimisel. Uuringu eesmärk on kaardistada administratiivtöötajate digiturvalisuse pädevuse enesetaju hetkeseis Eestis ja töötada välja hindamisvahend digiturvalisuse pädevuse mõõtmiseks.

Uuring on anonüümne ning Teie antud vastuseid ei isikustata. Kogutud andmeid kasutatakse uuringus üldistatult analüüsi läbiviimiseks.

Küsimuste korral pöörduge: 53806890 (Kaisa Niilo) või kaisa.niilo@tktk.ee

Aitäh!

Olge oma vastuses võimalikult objektiivne. Vältige soovmõtlemist.

Küsimused

- Hinda, mil määral järgnevad väited kehtivad sinu kohta (skaala 1 – üldse mitte, 5 – alati) (Ferrari, 2013) :

Küsimus	**Alati (5)**	**Sageli (4)**	**Mõnikord (3)**	**Harva (2)**	**Üldse mitte (1)**
Ma oskan kasutada põhivõtteid oma seadmete kaitsmiseks (nt viirusetõrje, salasõnad jms)					

Ma tean, et ma tohin enda ja teiste kohta e-keskkondades jagada ainult teatavat tüüpi infot					
Ma tean, kuidas vältida küberkiusamist					
Ma tean, et tehnoloogiliste vahendite väärkasutus võib kahjustada minu tervist					
Ma kasutan põhivõtteid energia säästmiseks					
Ma tean, kuidas oma digiseadmeid kaitsta					
Ajakohastan oma turvastrateegiaid, sh varundan oma tööfaile					
Ma kasutan alati kaheastmelist autentimist					
Ma oskan kaitsta enda ja teiste privaatsust e-keskkonnas					
Ma saan privaatsuse küsimustest üldiselt aru					
Mul on põhiteadmised selle kohta, kuidas minu andmeid kogutakse ja kasutatakse					

Ma tean, kuidas kaitsta ennast ja teisi küberkiusamise eest					
Mõistan tehnoloogiliste vahendite kasutamisega seotud terviseriske (alates ergonoomika aspektidest kuni tehnoloogiasõltuvuseni)					
Ma saan aru tehnoloogia kasutamise positiivsest ja negatiivsest mõjust keskkonnale					
Ma ajakohastan sageli oma turvastrateegiaid, sh väldin dubleerimist ja korrastan andmeid					
Ma oskan rakendada meetmeid, kui mu seade on ohus					
Ma muudan sageli e-teenuste vaikesätteid, et oma privaatsuse kaitset tõhustada					
Ma olen privaatsusküsimustega kursis, mul on selles valdkonnas laiad teadmised					
Ma tean, kuidas minu andmeid kogutakse ja kasutatakse					
Ma tean, kuidas kasutada tehnoloogilisi vahendeid nii, et vältida terviseprobleeme					

Ma tean, kuidas leida hea tasakaal e-maailma ja füüsilise maailma vahel					
Ma olen teadlik tehnoloogia mõjust igapäevaelule, veebitarbimisele ja keskkonnale					
Ma olen teadlik oma ettevõtte/organisatsiooni turvastrateegiast.*					
Minu tööarvuti on kaitstud tugeva salasõnaga ja ainult mina saan seda kasutada					
Kui ma installin internetist tarkvara oma tööarvutisse, siis kasutan tarkvara, mis kontrollib faili enne allalaadimist					
Kui ma kasutan info jagamiseks pilveteenuseid, krüptin konfidentsiaalset tööalast infot sisaldavad failid					
Ma tean, kuidas asutuses andmeid säilitatakse ja mis privaatsuspõhimõtteid rakendatakse					
Ma kontrollin sageli oma turvasätteid ja -meetmeid					

Kuna turvatarkvara uuendatakse automaatselt, siis ei pööra ma sellele tähelepanu					
Ma tean, kellega võimalike probleemide korral ühendust võtta					
Ma lülitan töölt lahkudes arvuti välja					
Ma mõistan, et minu vajadused uute seadmete järele võivad mõjutada keskkonda					
Ma uurin enne seadmete väljavahetamist töökohal, millised on parimad saadaolevad tehnoloogilised seadmed ja tarkvara					
Ma tean, et tööalaselt kasutatavad tehnoloogilised vahendid võivad tekitada sõltuvust, kuna neil on ka teisi kasutusotstarbeid					
Ma olen lugenud tehnoloogia negatiivsete ja positiivsete aspektide ning minu tööga seotud kasutusvõimaluste kohta; olen arutanud seda					

teemat veebis kolleegidega, kes töötavad samas valdkonnas					
Ma järgin oma ettevõtte/organisatsiooni turvastrateegiat.*					

Organisatsioonis, kus töötan, on olemas digitehnoloogia turvastrateegia ja tean selle sisu*

- On ja tean selle sisu.
- On aga sisuga pole tutvunud.
- Ei ole aga tunnen selle järgi suurt vajadust.
- Ei ole ega tunne ka puudust selle järgi.
- Ei oska öelda.

Vanus

- 18-24
- 25-34
- 35-49
- 50-64
- 65-74

Milline on Teie erialane haridus?

- Keskharidus
- Keskeriharidus
- Kutseharidus
- Rakenduslik kõrgharidus
- Bakalaureuse kraad
- Magistrikraad

Kas töötate era- või avalikus sektoris?

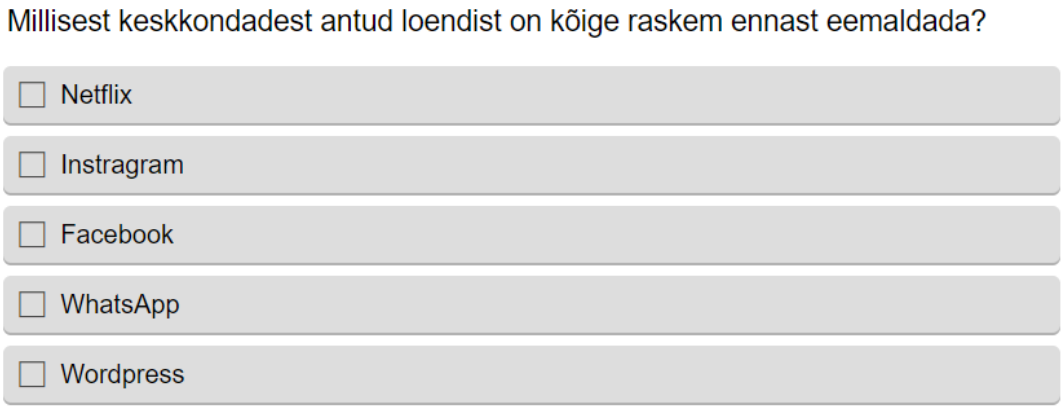
- Avalik sektor
- Erasektor

Piirkond kus elate

- Harjumaa
- Hiiumaa
- Ida-Virumaa
- Jõgevamaa
- Järvamaa
- Läänemaa
- Lääne-Virumaa
- Põlvamaa
- Pärnumaa
- Raplamaa
- Saaremaa
- Tallinn
- Tartumaa
- Valgamaa
- Viljandimaa
- Võrumaa

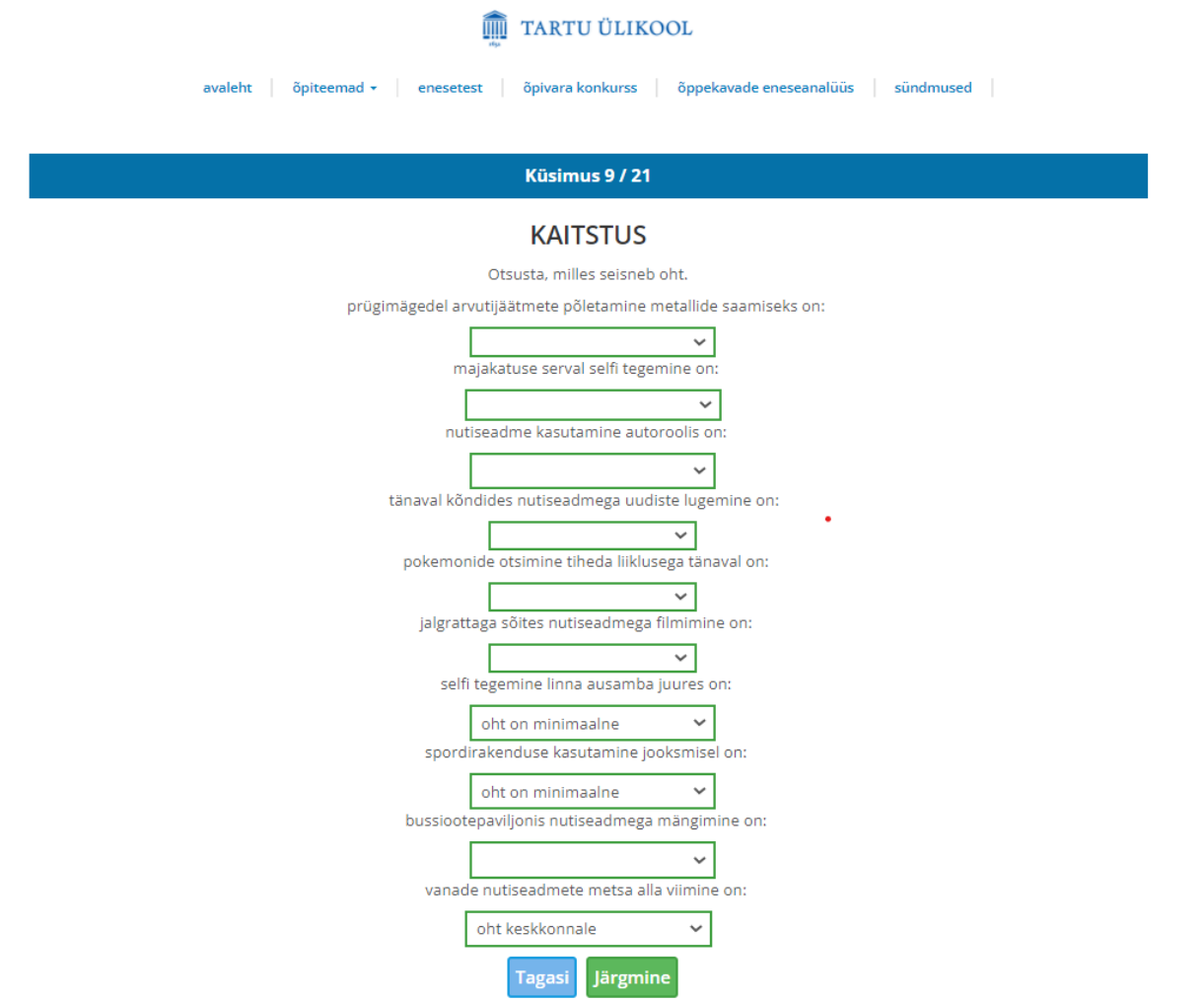
Lisa 2. Situatsioonülesanded

Situatsioonülesanne (privaatsussätted) 1 (Sõmer, Lorenz, Mäses & Muulmann):



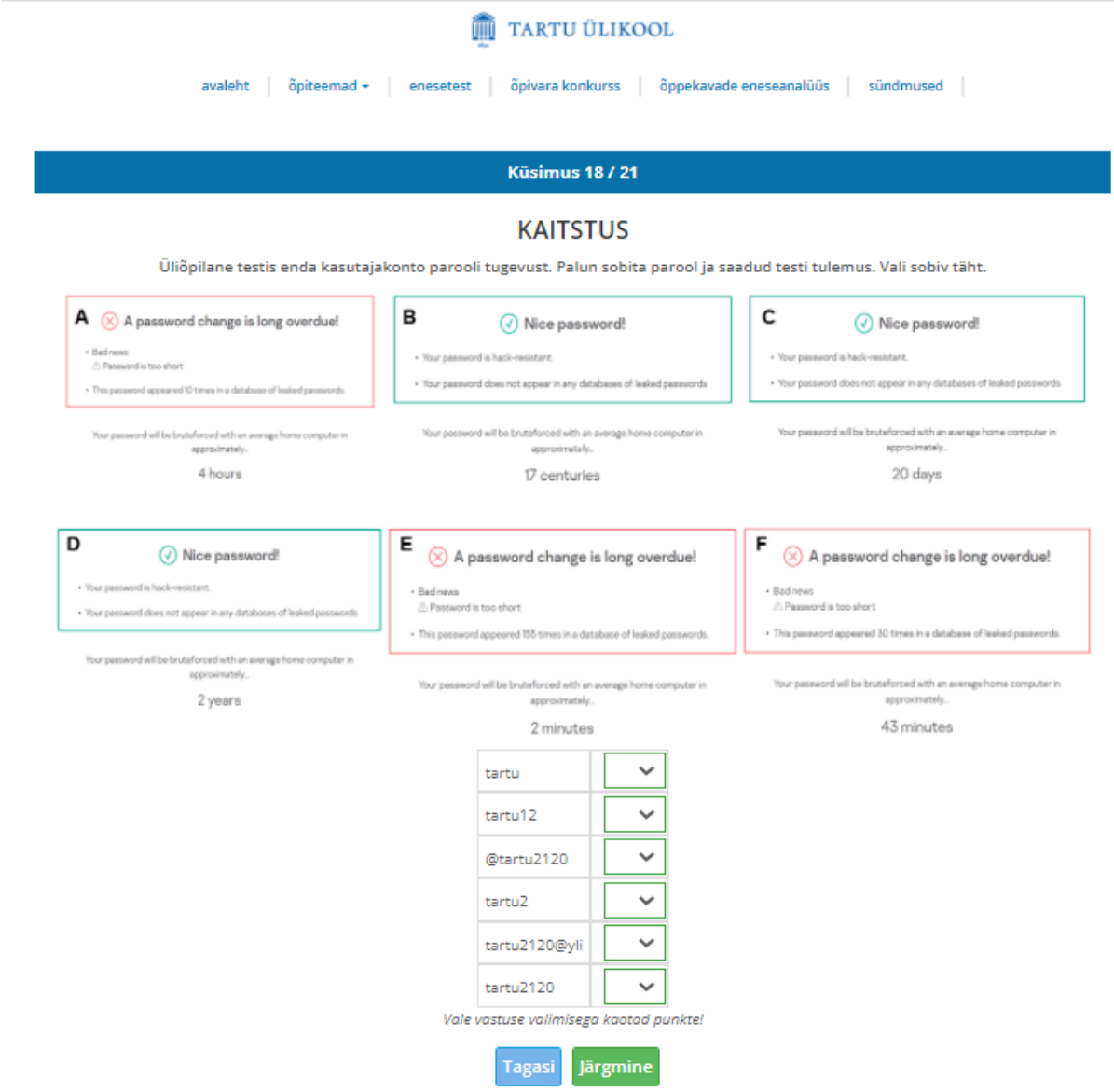
Joonis 12. Situatsioonülesanne 1 privaatsussätted kuvatõmmis

Situatsioonülesanne (oht tervisele ja keskkonnale) 2 (Tartu Ülikool)



Joonis 13. Situatsioonülesanne 2 kuvatõmmis

Situatsioonülesanne (salasõna tugevus) 3 (Tartu Ülikool):



Joonis 14. Situatsioonüleanne 3 parooli tugevuse hindamise kuvatõmmis

Situatsioonülesanne (oht) 4:

Ametlikku postkasti saabus kiri info@1hv.ee aadressilt, kus palutakse sisse logida aadressil http://www.1hv.ee kasutades kasutajatunnust ja parooli.

Vajutasid lingile ja valisid allalaadimise failil balance_sheet.bat

A) Avan ja käivitan faili, sest sellest võib selguda, faili päritolu.
B) Vajutan allalaadimise aknale, et fail ära kustutada.
C) Satun segadusse ja helistan IT toele, et olukord ära lahendada.

Lisa 3. Eesti õppijate digipädevusmudeli digiturvalisuse komponendi ja DigComp digiturvalisuse väidete võrdlus

4.4.10. eristab mõisteid “digitaalne jalajälg” ja “ökoloogiline jalajälg” ning oskab välja tuua nendevahelisi seoseid; 4.4.11. teeb põhjendatud otsuseid digitehnoloogiat valides (nt teavet luues ja tarbides, seadmeid ostes ja parandades); 4.4.12.teab, kuidas digitehnoloogiat toodetakse; 4.4.13. teab, kuidas digitehnoloogiat rakendatakse keskkonnakaitses; 4.4.14. sõnastab oma seisukoha ning seda toetavad argumendid digitehnoloogia ja keskkonna teemadel. 4.3.16. hindab digiseadmete kasutamisega seotud terviseriske alates ergonoomikast kuni arvutisõltuvuseni; 4.3.17. uurib ja analüüsib enda ja kaaslaste digiseadmete kasutamise harjumusi; 4.3.18. leiab tasakaalu digikeskkonna ja füüsilise keskkonna kasutamise vahel (online/offline tasakaal); 4.3.19. tunneb ära sekstimise (seksuaalse sõnumi saatmise) ja oskab hoiduda selle ohvriks sattumast; 4.3.20. mõistab digitehnoloogia ja sotsiaalse kaasatuse seoseid. 4.2.11. teab, mis on mitmeastmeline isikutuvastus ja seadistab oma kasutajakonto turvalisemaks; 4.2.12. teab, mis on andmekaitse üldmäärus (GDPR) ja tunneb oma õigusi, mis puudutavad andmete kogumist, hoiustamist ja kasutamist; 4.2.13. tunneb oma õigust olla unustatud, st oskab nõuda oma andmete kustutamist; 4.2.14. andmelekke korral teavitab juhendajat; 4.2.15. teab, mis on varikonto; 4.2.16. teeb vahet legaalsel ja illegaalsel tegevusel veebis; 4.2.17. mõistab identiteedivarguse ja muude isikuandmete varguse riski.	4.1. (A) Ma oskan kasutada põhivõtteid oma seadmete kaitsmiseks (nt viirusetõrje, salasõnad jms) 4.2. (A) Ma tean, et ma tohin enda ja teiste kohta e-keskkondades jagada ainult teatavat tüüpi infot 4.3 (A) Ma tean, kuidas vältida küberkiusamist 4.3 (A) Ma tean, et tehnoloogiliste vahendite väärkasutus võib kahjustada minu tervist 4.4. (A) Ma kasutan põhivõtteid energia säästmiseks 4.1. (B) Ma tean, kuidas oma digiseadmeid kaitsta 4.1. (B) Ajakohastan oma turvastrateegiaid, sh varundan oma tööfaile Ma kasutan alati kaheastmelist autentimist 4.2.(B) Ma oskan kaitsta enda ja teiste privaatsust e-keskkonnas 4.2. (B) Ma saan privaatsuse küsimustest üldiselt aru 4.2. (B) Mul on põhiteadmised selle kohta, kuidas minu andmeid kogutakse ja kasutatakse 4.3. (B) Ma tean, kuidas kaitsta ennast ja teisi küberkiusamise eest 4.3. (B) Mõistan tehnoloogiliste vahendite kasutamisega seotud terviseriske (alates ergonoomika aspektidest kuni tehnoloogiasõltuvuseni) 4.4. (B) Ma saan aru tehnoloogia kasutamise positiivsest ja negatiivsest mõjust keskkonnale 4.1. (C) Ma ajakohastan sageli oma turvastrateegiaid, sh väldin dubleerimist ja korrastan andmeid 4.1. (C) Ma oskan rakendada meetmeid, kui mu seade on ohus 4.2. (C) Ma muudan sageli e-teenuste vaikesätteid, et oma privaatsuse kaitset tõhustada 4.2. (C) Ma olen privaatsusküsimustega kursis, mul on selles valdkonnas laiad teadmised 4.2. (C) Ma tean, kuidas minu andmeid kogutakse ja kasutatakse

4.1.23. tunneb turvalisusega seotud mõisteid eesti ja inglise keeles (nt viirusetõrje, õngitsuskiri, tulemüür) ning teab erinevaid interneti ohte; 4.1.24. hindab veebikeskkonna või nutirakenduse turvalisust; 4.1.25. valib võimalusel sobiva wifi võrgu, millega on tagatud seadme ja andmete privaatsus; 4.1.26. teab, kuidas mobiilset internetti teiste seadmetega turvaliselt jagada (st wifi tulipunkti luua); 4.1.27. teab, mida teha või kelle poole pöörduda, kui digiseade on kahjustatud (arvutiviiruse, veekahjustuse vms tõttu); 4.1.28. teab, kuidas uuendada oma nutiseadme tarkvara ja paigaldada viirusetõrjet; 4.1.29. teeb oma andmetest regulaarselt varukoopiaid.	4.3. (C) Ma tean, kuidas kasutada tehnoloogilisi vahendeid nii, et vältida terviseprobleeme 4.3. (C) Ma tean, kuidas leida hea tasakaal e-maailma ja füüsilise maailma vahel 4.4. (C) Ma olen teadlik tehnoloogia mõjust igapäevaelule, veebitarbimisele ja keskkonnale Ma olen teadlik oma ettevõtte/organisatsiooni turvastrateegiast.* 4.1. (A) Minu tööarvuti on kaitstud tugeva salasõnaga ja ainult mina saan seda kasutada 4.1. (B) Kui ma installin internetist tarkvara oma tööarvutisse, siis kasutan tarkvara, mis kontrollib faili enne allalaadimist 4.1. (C) Kui ma kasutan info jagamiseks pilveteenuseid, krüptin konfidentsiaalset tööalast infot sisaldavad failid 4.2. (C) Ma tean, kuidas asutuses andmeid säilitatakse ja mis privaatsuspõhimõtteid rakendatakse 4.2. (C) Ma kontrollin sageli oma turvasätteid ja -meetmeid 4.2. (C) Ma tean, kellega võimalike probleemide korral ühendust võtta 4.4.(A) Ma lülitan töölt lahkudes arvuti välja 4.4. (B) Ma mõistan, et minu vajadused uute seadmete järele võivad mõjutada keskkonda 4.4. (C) Ma uurin enne seadmete väljavahetamist töökohal, millised on parimad saadaolevad tehnoloogilised seadmed ja tarkvara 4.3. (A) Ma tean, et tööalaselt kasutatavad tehnoloogilised vahendid võivad tekitada sõltuvust, kuna neil on ka teisi kasutusotstarbeid 4.4. (C) Ma olen lugenud tehnoloogia negatiivsete ja positiivsete aspektide ning minu tööga seotud kasutusvõimaluste kohta; olen arutanud seda teemat veebis kolleegidega, kes töötavad samas valdkonnas. Ma järgin oma ettevõtte/organisatsiooni turvastrateegiat.* Kuna turvatarkvara uuendatakse automaatselt, siis ei pööra ma sellele tähelepanu.*

Lisa 4. Korrelatsioonimaatriks

Correlations

			Vanus	Haridus	Kuna viimati läbisid mõne digiturvalisuse koolituse/õppepäeva/infotunni ?	Organisatsioonis, kus töötan, on olemas digitehnoloogia turvastrateegia ja tean selle sisu*.	Ma oskan rakendada meetmeid, kui mu seade on ohus	Ma oskan kaitsta enda ja teiste privaatsust e-keskkonnas	Ma uurin enne seadmete väljavahetamist töökohal, millised on parimad saadaolevad tehnoloogilised seadmed ja tarkvara	Minu tööarvuti on kaitstud tugeva salasõnaga ja ainult mina saan seda kasutada	Ma tean, kuidas kasutada tehnoloogilisi vahendeid nii, et vältida terviseprobleeme	SIT KOOND	Keskkondade lepingute sisu mõistmine	Tegevus kahtlase faili korral	Ma olen teadlik oma ettevõtte/organisatsiooni turvastrateegiast.*	Ma tean, kuidas oma digiseadmeid kaitsta	Kui ma installin internetist tarkvara oma tööarvutisse, siis kasutan tarkvara, mis kontrollib faili enne allalaadimist	Ma tean, kuidas asutuses andmeid säilitatakse ja mis privaatsuspõhimõtteid rakendatakse
Spearman's rho	Vanus	Correlation Coefficient	1.000	.185	.104	.121	.081	.088	.191	.007	.368*	-.338*	-.176	-.313*	-.015	.244	.170	.259
		Sig. (2-tailed)	.	.223	.495	.429	.595	.565	.210	.964	.013	.023	.249	.036	.921	.106	.265	.086
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Haridus	Correlation Coefficient	.185	1.000	-.105	.049	.019	-.151	.393**	.318*	.358*	.151	-.058	-.324*	.036	.189	.258	.263
		Sig. (2-tailed)	.223	.	.493	.749	.904	.322	.008	.033	.016	.321	.704	.030	.816	.214	.088	.081
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Kuna viimati läbisid mõne digiturvalisuse koolituse/õppepäeva/infotunni ?	Correlation Coefficient	.104	-.105	1.000	.549**	.405**	.502**	.029	.206	-.003	.064	.238	-.234	.496**	.386**	.133	.145
		Sig. (2-tailed)	.495	.493	.	<.001	.006	<.001	.851	.174	.982	.676	.115	.122	<.001	.009	.384	.343
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Organisatsioonis, kus töötan, on olemas digitehnoloogia turvastrateegia ja tean selle sisu*.	Correlation Coefficient	.121	.049	.549**	1.000	.266	.249	.052	.392**	.101	.054	-.019	-.230	.563**	.325*	.215	.445**
		Sig. (2-tailed)	.429	.749	<.001	.	.077	.100	.733	.008	.510	.724	.902	.128	<.001	.029	.155	.002
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Ma oskan rakendada meetmeid, kui mu seade on ohus	Correlation Coefficient	.081	.019	.405**	.266	1.000	.589**	.211	.228	.247	.152	.071	-.346*	.328*	.612**	.171	.451**
		Sig. (2-tailed)	.595	.904	.006	.077	.	<.001	.165	.132	.102	.320	.645	.020	.028	<.001	.262	.002
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Ma oskan kaitsta enda ja teiste privaatsust e-keskkonnas	Correlation Coefficient	.088	-.151	.502**	.249	.589**	1.000	.198	.185	.093	-.108	-.033	-.277	.403**	.566**	.228	.215
		Sig. (2-tailed)	.565	.322	<.001	.100	<.001	.	.193	.224	.543	.479	.831	.066	.006	<.001	.131	.156
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Ma uurin enne seadmete väljavahetamist töökohal, millised on parimad saadaolevad tehnoloogilised seadmed ja tarkvara	Correlation Coefficient	.191	.393**	.029	.052	.211	.198	1.000	.143	.287	-.004	.038	-.240	.167	.280	.236	.330*
		Sig. (2-tailed)	.210	.008	.851	.733	.165	.193	.	.350	.056	.979	.803	.112	.272	.063	.119	.027
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Minu tööarvuti on kaitstud tugeva salasõnaga ja ainult mina saan seda kasutada	Correlation Coefficient	.007	.318*	.206	.392**	.228	.185	.143	1.000	.267	.140	.171	-.158	.439**	.127	.360*	.369*
		Sig. (2-tailed)	.964	.033	.174	.008	.132	.224	.350	.	.076	.358	.260	.300	.003	.406	.015	.013
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Ma tean, kuidas kasutada tehnoloogilisi vahendeid nii, et vältida terviseprobleeme	Correlation Coefficient	.368*	.358*	-.003	.101	.247	.093	.287	.267	1.000	-.191	.089	-.439**	.089	.380*	.247	.549**
		Sig. (2-tailed)	.013	.016	.982	.510	.102	.543	.056	.076	.	.210	.561	.003	.561	.010	.102	<.001
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	SIT KOOND	Correlation Coefficient	-.338*	.151	.064	.054	.152	-.108	-.004	.140	-.191	1.000	-.064	.067	.135	.066	-.074	.070
		Sig. (2-tailed)	.023	.321	.676	.724	.320	.479	.979	.358	.210	.	.675	.660	.378	.665	.627	.650
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Keskkondade lepingute sisu mõistmine	Correlation Coefficient	-.176	-.058	.238	-.019	.071	-.033	.038	.171	.089	-.064	1.000	.193	-.173	-.239	.198	-.087
		Sig. (2-tailed)	.249	.704	.115	.902	.645	.831	.803	.260	.561	.675	.	.204	.257	.113	.193	.572
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Tegevus kahtlase faili korral	Correlation Coefficient	-.313*	-.324*	-.234	-.230	-.346*	-.277	-.240	-.158	-.439**	.067	.193	1.000	-.293	-.554**	-.339*	-.436**
		Sig. (2-tailed)	.036	.030	.122	.128	.020	.066	.112	.300	.003	.660	.204	.	.050	<.001	.023	.003
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Ma olen teadlik oma ettevõtte/organisatsiooni turvastrateegiast.*	Correlation Coefficient	-.015	.036	.496**	.563**	.328*	.403**	.167	.439**	.089	.135	-.173	-.293	1.000	.445**	.074	.509**
		Sig. (2-tailed)	.921	.816	<.001	<.001	.028	.006	.272	.003	.561	.378	.257	.050	.	.002	.628	<.001
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Ma tean, kuidas oma digiseadmeid kaitsta	Correlation Coefficient	.244	.189	.386**	.325*	.612**	.566**	.280	.127	.380*	.066	-.239	-.554**	.445**	1.000	.311*	.433**
		Sig. (2-tailed)	.106	.214	.009	.029	<.001	<.001	.063	.406	.010	.665	.113	<.001	.002	.	.038	.003
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Kui ma installin internetist tarkvara oma tööarvutisse, siis kasutan tarkvara, mis kontrollib faili enne allalaadimist	Correlation Coefficient	.170	.258	.133	.215	.171	.228	.236	.360*	.247	-.074	.198	-.339*	.074	.311*	1.000	.226
		Sig. (2-tailed)	.265	.088	.384	.155	.262	.131	.119	.015	.102	.627	.193	.023	.628	.038	.	.136
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45
	Ma tean, kuidas asutuses andmeid säilitatakse ja mis privaatsuspõhimõtteid rakendatakse	Correlation Coefficient	.259	.263	.145	.445**	.451**	.215	.330*	.369*	.549**	.070	-.087	-.436**	.509**	.433**	.226	1.000
		Sig. (2-tailed)	.086	.081	.343	.002	.002	.156	.027	.013	<.001	.650	.572	.003	<.001	.003	.136	.
		N	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).