TARTU ÜLIKOOLI VILJANDI KULTUURIAKADEEMIA

Kunstide ja tehnoloogia
õpetaja

German Jaska

ESMAKURSUSLASTE KÜBERTURVALISUSE TEADLIKKUS JA SUHTUMISED KOLME EESTI KÕRGKOOLI NÄITEL

Magistritöö

Juhendaja: Meeli Rannastu-Avalos, MSc,
haridustehnoloogia nooremlektor

Viljandi 2024

RESÜMEE

Esmakursuslaste küberturvalisuse teadlikkus ja suhtumised kolme eesti kõrgkooli näitel

Kaasaegses maailmas, kus tehnoloogia areneb kiiresti ja selle levik igapäevaelus aina suureneb, kasvab ka sellega seotud küberturvalisuse ohtude hulk. Teadlikkuse tõstmine küberturvalisuse osas on kriitilise tähtsusega, et ennetada riske ja reageerida ohtudele õigeaegselt. Efektiivne viis selle eesmärgi saavutamiseks on aktiivne teavitustöö ja küberturvalisuse teemade kaasamine koolide ja ülikoolide õppekavadesse. Käesolev magistritöö keskendub digipädevuse ja küberturvalisuse teadlikkuse uurimisele Eesti ülikoolide esmakursuslaste seas. Uurimuse peamised eesmärgid hõlmavad õpilaste enesehindamise analüüsi oma teadmiste ja küberturvalisuse põhimõtete ning riskide tajumise osas ning nende suhtumise uurimist küberturvalisuse tähtsuse ja oma rolli mõistmises digitaalses turvalisuses. Uuring viidi läbi kvantitatiivse analüüsi vormis, kasutades struktureeritud küsimustikku, mis oli suunatud tudengite teadmiste ja suhtumise hindamisele küberturvalisuse valdkonnas.

Märksõnad: küberturvalisus, nutiseadmed, digipädevus, kõrgharidus

SISUKORD

SISSEJUHATUS

Digiajastul, kus digitaalne dimensioon põimub iga inimeste igapäevaelu aspektiga, tõuseb digipädevuse omandamine esile kui hädavajalik tingimus edu saavutamiseks sotsiaalses, professionaalses ja isiklikus sfääris (Harno, 2023). Eesti, mis on tunnustatud ühe digiinnovatsiooni liidrina Euroopa Liidus, on juba üle kümne aasta näidanud püüdlust tagada usaldusväärne küberjulgeolek, eesmärgiga garanteerida rahvuslike institutsioonide ja kriitilise tähtsusega teenuste kaitse ja kättesaadavus igas olukorras (Vaks, 2013). Selles kontekstis muutuvad digipädevuse ja küberjulgeoleku küsimused eriti aktuaalseks ja võtavad riigi haridusagendas juhtiva koha (RIA, 2023). Siiski, kasvav uudisvoog ja arutelud noorte seas näitavad, et digitaalse turvalisuse ja hügieeni probleemid puudutavad üha enam noort põlvkonda, tõstes esile riske ja väljakutseid, millega nad digiruumis silmitsi seisavad. See digitaalse turvalisuse teema aktualiseerimine ja selle resonants noorte seas on mind tõuganud viima läbi haridusteaduslikku uurimistööd selles valdkonnas.

Käesoleva uuringu peamised eesmärgid on hinnata, kuidas Eesti ülikoolide esmakursuslased oma digipädevust küberjulgeoleku kontekstis mõistavad, eriti seoses nutiseadmete kasutamisega. Uuring põhineb kooli digipädevuse programmi (Vuorikari *et al.*, 2022) süsteemil ja keskendub tudengite teadlikkusele ning suhtumisele küberjulgeoleku riskide ületamiseks. Uuringu uurimisküsimused on järgmised:

1. Nutiseadmete küberturvalisuse teadlikkuse hindamine: Kuidas Eesti ülikoolide esmakursuslased hindavad oma teadmisi küberturvalisuse põhimõtetest ja riskidest nutiseadmete kontekstis.

2. Nutiseadmete küberturvalisuse suhtumise analüüs: Kuidas üliõpilased mõistavad küberturvalisuse tähtsust ja oma rolli nutiseadmete turvalisuse tagamisel.

Selle lähenemise abil saab tuvastada võimalikud lüngad tudengite teadmistes ja suhtumises, mis võimaldab paremini kohandada õppekavasid nende vajadustele. Uuring on suunatud mõistmisele, kui ulatuslikud on koolis omandatud teadmised ja oskused ning kas need rakenduvad tudengite poolt reaalsetes küberjulgeoleku ja -hügieeni stsenaariumides. See aitab kaasa tõhusamate haridusstrateegiate väljatöötamisele, et parandada tudengite küberjulgeoleku taset ja valmistada neid ette edukaks toimetulekuks kaasaegse digimaailma väljakutsetega. Saadud tulemused on olulised nii õppekavade koostajatele ja spetsialiseeritud

kursuste õpetajatele kui ka laiemalt haridussektori huvigruppidele. Uuringu tulemused on üksikasjalikult välja toodud töö peatükis "Tulemused".

1. TEOREETILINE ÜLEVAADE

Järgnevas sissejuhatuses antakse ülevaade peatükkide sisust, mis keskenduvad erinevatele aspektidele, seotud nutiseadmete ja küberturvalisusega. Esimeses peatükis keskendutakse eelkõige nutiseadmete määratlusele, nende peamistele omadustele, nagu asjakohasus, interaktiivsus ja üldine ülevaade probleemidest. Käsitletakse nende rolli kaasaegses ühiskonnas ja erilisi väljakutseid, mida nad küberturvalisuse kontekstis esitavad.

Teises peatükis analüüsitakse digipädevuse kontseptsiooni ja selle olulisust riiklikus õppekavas. Käsitletakse Eesti praeguseid standardeid ja ootusi üliõpilaste digipädevuse tasemele, samuti meetodeid ja strateegiaid nende parandamiseks haridusprotsessis.

Kolmandas jaos keskendutakse küberturvalisusele ja nutiseadmetega seotud peamistele riskidele. Arutletakse erinevate ohtude üle, sealhulgas pahavara, andmepüük, andmete vargus ja muud rünnakute vektorid, samuti strateegiad nende riskide minimeerimiseks.

Viimane osa pakub ülevaadet olemasolevatest uurimustest küberturvalisuse teadlikkuse mõõtmise ja hindamise teemal. Selles osas analüüsitakse erinevaid kvantitatiivseid meetodeid, kaasa arvatud küsitlusi ja teste, mis on kasutatud teadmiste ja teadlikkuse hindamiseks selles valdkonnas.

1.1 Nutiseadmete mõiste ja kontseptsioonid

Kaasaegne maailm muutub üha digitaalsemaks ja omavahel seotumaks, mis viib märkimisväärsele kasvule nutistu ehk asjade interneti (inglise keeles Internet of Things, lühend IoT) ja nutiseadmete kasutamises (Erelt *et al.,* 2014; Sharma & Sharma, 2020). Interneti asjade (IoT) mõiste hõlmab integreeritud objektide võrku, mis katab laia valikut seadmeid alates lihtsatest anduritest kuni keerukamate seadmeteni, nagu nutitelefonid ja tahvelarvutid (Lueth, 2014; Madakam, 2015; Kouroupis, 2023). See kontseptsioon on suhteliselt uus kaasaegsete traadita telekommunikatsiooni valdkonnas ja näitab kiiret kasvu, prognoosidega seotud seadmete arvu suurenemisest (Madakam, 2015; Risteska Stojkoska &

Trivodaliev, 2017). 2023. aasta alguse seisuga kasutab nutitelefone 5,44 miljardit inimest, mis moodustab 68% maailma rahvastikust. Erinevate kasutajate arv jätkab kasvamist igal aastal, ületades juba 5 miljardit sotsiaalvõrgustike kasutajat (Global Digital, 2023).

Asjade interneti (IoT) kontseptsiooni rakendatakse erinevates sektorites, luues uusi võimalusi ja mängides olulist rolli turukonkurentsi määrajana (Madakam, 2015). See tehnoloogia annab märkimisväärse panuse nii maailmatööstuse sisemiste kui ka väliste protsesside parendamisele, soodustades innovaatilist arengut ja tõhususe tõstmist (Gartner, 2016; Madakam, 2015). Selle paradigma laienemine on toonud kaasa mitmesuguste ja mõnikord vastuoluliste terminite kasutamise teaduskirjanduses, et tähistada seadmeid, mis kuuluvad asjade interneti koosseisu (Lueth, 2014). Sellisteks terminiteks on "mobiilsed seadmed", "nutiseadmed", "mobiiltehnoloogiad" ja "mobiilsed nutiseadmed" (Erelt *et al.,* 2014). See terminoloogia mitmekesisus peegeldab asjade interneti kontseptsiooni arengut ja evolutsiooni akadeemilises ja teaduslikus kontekstis (Whitmore, 2015).

Asjade internet (IoT) areneb kiiresti ja omab suurt potentsiaali hariduse valdkonnas, pakkudes tõhusat digitaalsete süsteemide haldamist ning andmete reaalajas kogumist ja analüüsi (Kurzweil & Baker, 2017). Akadeemilistes ringkondades on täheldatav suurenev huvi kantavate mobiilseadmete vastu, mis on seotud asjade internetiga (IoT). Siiski on see huvi piiratud küberturvalisusega seotud murede tõttu, kuna sellised seadmed on sageli haavatavad andmete privaatsuse rikkumiste ja turvakaitse probleemide suhtes. Lisaks on piiratud ressursside tõttu puudus uuringutest, mis käsitleksid kantavate seadmete tõhusat kasutamist professionaalses tegevuses ja akadeemilistes uurimustes (KeeJoh O'Hearon et al., 2021; Sam et al., 2020). See toob vajadus kohandada ja integreerida haridusprogramme, võttes arvesse andmekaitsega seotud probleeme ja riske. Samuti on oluline arvestada õigusliku ja tehnilise kontekstiga (KeeJoh O'Hearon *et al*., 2021; Kouroupis & Vagianos, 2023).

Uuringus, mille viisid läbi Lopez jt (2017), töötati välja kontseptuaalne mudel, mis koosneb kolmest põhilisest komponendist, mis on vajalikud asjade interneti (IoT) paradigma rakendamiseks. Need komponendid hõlmavad endas nutiseadmeid, võrguinfrastruktuuri ja serverilahendusi (Lopez *et al.,* 2017).

Mudeli järgi on nutiseadmed, mis suudavad suhelda, mõeldud interaktsiooniks nii lõppkasutajatega kui ka teiste võrku ühendatud seadmetega. Täheldatud on, et mõned neist seadmetest võivad toimida autonoomselt, ilma vajaduseta kasutaja otsest juhtimist. Seega

kujutab see lihtsustatud arhitektuur endast raamistruktuuri asjade interneti süsteemide väljatöötamiseks ja toimimiseks (Lopez *et al.,* 2017).

Nutiseadmed on elektroonilised seadmed, millel on täiustatud arvutusvõimed, võrguühendus ja suutlikkus suhelda kasutaja või teiste seadmetega. Need omavad tihti automaatse uuendamise võimalust ja kohanduvad uute tingimustega tänu sisseehitatud tarkvarale ja tehisintellektile.

Süstemaatilise kirjandusanalüüsi käigus tuvastati nutiseadmete peamised omadused, mida teadustöödes mainitakse. Nende hulka kuuluvad autonoomia, ühenduvus, kontekstiteadlikkus, kasutajaga suhtlemine, mobiilsus ja andmete salvestamine (Silverio-Fernández, 2018). Uuring (Risteska Stojkoska & Trivodaliev, 2017) näitas, et ühenduvus ja kasutajaga suhtlemine on kõige sagedamini mainitud omadused, kuid neid kõiki ei peeta IoT kontseptsiooni jaoks võtmetähtsusega.

Seega võib "nutiseadme" peamisi omadusi asjade interneti (IoT) raames kirjeldada järgmiselt:

• Autonoomia: Nutiseadmed on võimelised autonoomselt ülesandeid täitma ilma inimese pideva sekkumiseta. Nad on varustatud sisseehitatud andmetöötlusalgoritmidega, mis võimaldavad neil otsuseid langetada kogutud andmete põhjal.

• Ühenduvus: Need seadmed suudavad ühenduda teiste seadmetega või võrkudega andmete vahetamiseks. Ühendus võib olla nii juhtmega kui ka juhtmeta ning sageli hõlmab see internetiühendust, mis võimaldab seadet integreerida laiemasse IoT-võrku.

• Kontekstiteadlikkus: Nutiseadmed on võimelised tajuma ja analüüsima teavet oma keskkonnast. Nad on varustatud andurite ja teiste andmekogumismehhanismidega, nagu kaamerad, mikrofonid, GPS-modulid ja kiirendusmõõturid, mis võimaldavad neil kohaneda keskkonnamuutustega ja reageerida neile asjakohaselt.

Need põhiomadused määravad nutiseadmete käitumise ja funktsionaalsuse kaasaegses IoT ökosüsteemis. Vastavalt Silverio-Fernándezi (2018) uuringu järeldustele eelistatakse käesolevas töös terminit "nutiseadmed" telefonide, tahvelarvutite ja teiste nutiseadmete tähistamiseks, millega üliõpilased suhtlevad. See valik on tingitud selle termini vastavusest kaasaegsetele kontseptsioonidele ja nutiseadmete omadustele (Silverio-Fernández, 2018).

1.2 Digipädevus ja pädevused riiklikus õppekavas

Peatükk võtab kokku digipädevuse olulisuse tänapäeva hariduselus, kus tehnoloogiline areng ja digitaalsete vahendite kasutamine on igapäevane reaalsus. Eesti haridussüsteemis on digipädevus tunnistatud kriitiliseks oskuseks, mis võimaldab inimestel toime tulla kiiresti muutuvas ühiskonnas, olles integreeritud osa riiklikust õppekavast.

Õppekava on haridusprotsessi põhidokument, mis sätestab õppe- ja kasvatuseesmärgid, määratleb õppematerjalide sisu ja mahu, õpetamise metoodika alused, õpilaste saavutuste hindamise kriteeriumid ning hariduskeskkonna standardid ja muud seotud aspektid. See dokument on aluseks haridusprogrammide süstemaatilisele rakendamisele kõikidel haridustasemetel (HAR, 2014).

Käesoleva uurimistöö raames kasutatakse terminit "õppekava" struktureeritud õppeprogrammi kirjeldamiseks, mis on kasutusel mitmesugustes haridusasutustes, sealhulgas üldhariduskoolides, kõrgkoolides ja täiendõppe keskustes, nagu kutsealased koolituskursused. Selles kontekstis on õppekava kompleksne plaan, mis on suunatud eelnevalt määratletud hariduseesmärkide ja -standardite saavutamisele organiseeritud õppe kaudu, mis on kohandatav erinevatele haridustasemetele ja õppevormidele.

See hõlmab laia spektrit teadmisi ja oskusi, alates infootsingust ja digitaalse sisu loomisest kuni digitaalsete vahendite turvalise kasutamiseni. Euroopa Liidu DigComp raamistiku järgi arendatud Eesti õppijate digipädevusmudel rõhutab digipädevuse mitmekülgsust ja selle olulisust õpilaste isiklikus arengus, tööhõives, sotsiaalses kaasatuses ja aktiivses kodanikuühiskonnas osalemises. Digipädevus on tänapäeva haridusmaailmas muutunud üha olulisemaks oskuseks, arvestades kiiret tehnoloogilist arengut ja digitaalsete vahendite kasutamise suurenemist igapäevaelus. Digipädevuse mõiste hõlmab mitmeid olulisi oskusi ja teadmisi, mis on vajalikud digitaalsete tehnoloogiate tõhusaks ja turvaliseks kasutamiseks (Vuorikari *et al.*, 2022).

Eesti haridussüsteemis on digipädevust määratletud kui suutlikkust kasutada digitehnoloogiat toimetulekuks kiiresti muutuvas ühiskonnas nii õppimisel, kodanikuna tegutsedes kui ka kogukondades suheldes (Harno, 2017; Vuorikari *et al.*, 2022). Digipädevus on muutunud üheks nendest olulistest pädevustest, mis on integreeritud riiklikku õppekavasse erinevates ainetes ja tasemetel. Selle eesmärk on tagada, et õpilased omandaksid vajalikud digipädevused edukaks toimetulekuks tänapäeva digitaalses maailmas (Harno, 2023).

Eesti õppijate digipädevusmudel põhineb Euroopa Komisjoni välja antud rahvusvahelisel digipädevuse raamistikul. Euroopa Liidu DigComp digipädevuse raamistikus kirjeldatakse digipädevust kui teadmiste, oskuste ja võimete kogumit, mis on vajalikud digitaaltehnoloogiate efektiivseks ja kriitiliseks kasutamiseks. See hõlmab ohutut ja eetilist suhtlemist digitaalses maailmas ning katab erinevaid aspekte, sealhulgas teabe otsimist, töötlemist ja hindamist, vahendite kasutamist digitaalse sisu loomiseks, suhtlemist ja koostööd digitaalsetes keskkondades ning arusaamist ja osalemist digitaalses kirjaoskuses ja turvalisuses. See on keerukas mõiste, mis on oluline isikliku arengu, tööhõive, sotsiaalse kaasatuse ja aktiivse kodanikuühiskonna osalemise jaoks (Vuorikari *et al.*, 2022).

Digipädevuse raamistiku "Turvalisuse" komponent sisaldab nelja peamist valdkonda (Vuorikari *et al.*, 2022):

1. Seadmete kaitse: Seadmete ja digitaalse sisu turvalisuse tagamine, digitaalse keskkonna riskide ja ohtude mõistmine, turva- ja privaatsusmeetmete tundmine.

2. Isikuandmete ja privaatsuse kaitse: Isikuandmete kaitsmine digitaalsetes keskkondades, arusaamine, kuidas isikuandmeid kasutada ja jagada, enda ja teiste kaitsmine kahju eest.

3. Tervise ja heaolu kaitse: Digitaaltehnoloogiate kasutamisel terviseriskide vältimine ja psühholoogilise heaolu kaitse, digitaalses keskkonnas esinevate ohtude, nagu küberkiusamine, eest kaitsmine.

4. Keskkonna kaitse: Teadlikkus digitaaltehnoloogiate mõjust keskkonnale ja nende kasutamine.

Põhikooli ja gümnaasiumi riiklikud õppekavad (GRÕK, 2023) kirjeldavad digipädevust kui olulist pädevust, mis on vajalik õpilastele nende haridustee jooksul. Need pädevused hõlmavad järgmisi valdkondi:

1. Infootsing ja hindamine: õpilased peaksid suutma leida ja hinnata infot digivahendite abil ning mõistma selle asjakohasust ja usaldusväärsust.

2. Digitaalse sisuloomes osalemine: õpilased peaksid oskama osaleda digitaalses sisuloomes, luues ja kasutades tekste, pilte ja multimeediumi.

3. Probleemilahendus ja koostöö digikeskkonnas: õpilased peaksid oskama kasutada digivahendeid probleemide lahendamiseks ja suhtlemiseks digitaalsetes keskkondades.

4. Digikeskkonna ohutus: õpilased peaksid olema teadlikud digikeskkonna ohtudest ning oskama kaitsta oma privaatsust, isikuandmeid ja digitaalset identiteeti.

5. Eetika ja väärtused digikeskkonnas: õpilased peaksid järgima digikeskkonnas samu moraali- ja väärtuspõhimõtteid nagu igapäevaelus.

1.3 Küberturvalisuse riskid nutiseadmete kontekstis

Tehnoloogiate arenguga on tunnistajaks revolutsioonilistele muutustele paljudes elu aspektides. Ühendatud seadmete arvu kasvades suureneb ka võimalike haavatavuste arv (Lella, 2023). Paljude asjade interneti seadmete projekteerimisel keskendutakse mugavusele ja funktsionaalsusele, kuid alati ei pöörata piisavalt tähelepanu turvalisusele, eetikale ja tarkvara haavatavustele (Rikk, 2018). Nutiseadmed, mis on muutunud õpilaste kaasaegse elu lahutamatuks osaks, kujutavad endast potentsiaalset küberturvalisuse ohtu (Mai & Tick, 2021).

Küberturvalisus on tööriistade, poliitikate, turvamõistete, turvakaitsevahendite, juhendite, riskijuhtimisviiside, tegevuste, koolituste, parimate praktikate, kinnituste ja tehnoloogiate kogum, mida saab kasutada kübersfääri ja organisatsiooni ning kasutajate varade kaitsmiseks. Organisatsiooni ja kasutajate varad hõlmavad ühendatud arvutiseadmeid, personali, taristut, rakendusi, teenuseid, telekommunikatsiooni ning kogu kübersfääris edastatud või talletatud informatsiooni (Rao, 2023).

Küberturvalisuse tähtsust ei saa alahinnata, kuna küberturvalisuse ohud kujutavad endast olulist ohtu üksikisikutele, organisatsioonidele ja valitsustele üle kogu maailma. See on eriti oluline, arvestades "nutiseadmete" (IoT - Internet of Things) laialdast levikut, mis suurendavad rünnakute sisenemispunkte ja nõuavad võrgu- ja seadmete turvalisuse suurendamist.

Küberturvalisuse ohud võivad esineda erinevatel kujudel, sealhulgas pahavara (viirused, ussid, Trooja hobused ja nuhkvara), õngitsemine, sotsiaalne manipuleerimine, teenusetõkestamise rünnakud (DDoS) ja pikaajalised sihipärased rünnakud (APT). Seetõttu peavad küberturvalisuse strateegiad hõlmama mitmeid kaitsekihte, mis on jaotatud üle kõigi ettevõtte arvutite, programmide ja võrkude (Rao, 2023).

Seega, arvestades nutiseadmete konteksti, muutub küberturvalisuse tagamine veelgi keerukamaks suure hulga andmete tõttu, mida need koguvad ja edastavad. Need seadmed on sageli sihtmärkideks küberrünnakutele, kuna neil on juurdepääs suurtele kogustele isiklikule teabele. Küberturvalisus peab kohanema pidevalt muutuva tehnoloogia- ja ohumaastikuga, uuendades kaitsepraktikaid nende ohtude vastu (Rao, 2023).

Küberjulgeoleku kontseptsiooni tähenduse kadumine erinevate valdkondade ekspertide seas toob esile vajaduse selgitada küberjulgeoleku mõistet, kuna selle tähtsuse ja arengutaju erinevused on olulised probleemid. Määratledes küberkindluse kui osa laiemast omaduste rühmast, mida nimetatakse "vastupidavuseks" (hõlmab vastupanuvõimet, vastupidavust, järjekindlust ja sitkust), on võimalik rakendada struktureeritumat ja keskendunumat lähenemisviisi (Smith, 2023). Selline kategoriseerimine aitab mõista, kuidas küberüsteemid ja kasutajad reageerivad stressile ja taastuvad sellest, mõjutades nende jõudlust. Selle määratluse kehtestamine on kriitilise tähtsusega täpsete mõõdikute ja meetodite väljatöötamiseks küberkindluse kvantitatiivseks hindamiseks, mis aitab paremini hallata ja suurendada küberüsteemide usaldusväärsust (Smith, 2023).

Selles uuringus püüame järgida varasemat määratlust, mille kohaselt küberjulgeolek on praktikate, tehnoloogiate, poliitikate ja meetmete kogum, mis on mõeldud võrkude, seadmete, programmide ja andmete kaitsmiseks rünnakute, kahjustuste või volitamata juurdepääsu eest (Skarga-Bandurova *et al.,* 2021).

Küberhügieen on küberjulgeoleku paradigma, mis rõhutab ennetavate meetmete ja ohutuskultuuri tähtsust organisatsioonides, et suurendada nende vastupanuvõimet küberohtudele. See lähenemine hõlmab teatud standardite ja praktikate süstemaatilist rakendamist ja järgimist, et kaitsta infoturbe süsteeme ja andmeid. Põhinedes organisatsioonikultuuri ja hariduse põhimõtetel, on küberhügieen suunatud riskide minimeerimisele ja konfidentsiaalse teabe kaitse tugevdamisele regulaarsete hinnangute, personali koolitamise ja turvajuhtimise protsesside täiustamise kaudu (Skarga-Bandurova *et al.,* 2021).

Eksperdid märgivad, et interneti populaarsuse kasvuga on küberkuritegevus muutunud tõsiseks probleemiks üksikisikutele, organisatsioonidele ja riikidele. Teave häkkerirünnakute, andmevarguste ja muude küberkuritegevuse vormide levik tekitab muret ja ärevust uute tehnoloogiate pärast, mida nüüd klassifitseeritakse küberkuritegudena (Chang & Coppel, 2020). Näiteks Eestis Riigi Infosüsteemi Ameti poolt töödeldud intsidentide aruande kohaselt

oli 2022. aastal registreeritud pöördumiste arv 27 115, mis näitab keskmist 74 pöördumist päevas. Nendest märkimisväärne osa (2672 juhtumit) puudutas intsidente, mis rikkusid informatsioonisüsteemide konfidentsiaalsust, terviklikkust või kättesaadavust. Märkimisväärselt suurenes phishing-rünnakute arv 1206 juhtumini, mis on kaks korda rohkem kui 2021. aastal (RIA, 2023).

Need andmed rõhutavad küberjulgeoleku teadlikkuse probleemi aktuaalsust kõigi kasutajakategooriate seas, eriti kooliõpilaste ja üliõpilaste hulgas. Samuti tuleks tähelepanu pöörata kriitilise mõtlemise oskuste arendamisele ja internetis oleva teabe hindamisele, samuti teadliku ja turvalise käitumise kujundamisele võrgus (Bada *et al.,* 2015).

Digitaalajastul ja ülemaailmse ühenduvuse ajastul muutub Interneti asjad üha integreeritumaks igapäevaelus, mis toob kaasa küberrünnakute kasvu (ENISA, 2023) aasta aruande kohaselt seisab maailm silmitsi küberrünnakute mitmekesisuse ja mahu järsu suurenemisega, sealhulgas pettused, mis kasutavad sotsiaalset inseneri ja ründeid, mis on suunatud andmetele ja teenuste kättesaadavusele.

Tuleb märkida, et märtsis 2024 toimus Eesti riigisektori internetiressursside vastu suunatud küberrünnak, mis oma ulatuselt ei ole leidnud analooge. Riigi Infosüsteemi Ameti juures tegutsev küberrünnete reageerimise üksus, tuntud kui CERT-EE, registreeris kevade esimesel kuul rekordarvu tõsiseid küberründejuhtumeid, ületades 500 juhtumit (RIA, 2024). Selline näitaja on viimaste aastate kõrgeim. Nende rünnakute peamiseks eesmärgiks oli pangakaartide andmete ebaseaduslik omastamine, samuti kasutajate sisselogimisandmete ja paroolide vargus (RIA, 2024). Selline olukord rõhutab riiklike institutsioonide tasandil küberturvalisuse mehhanismide pideva analüüsi ja tugevdamise tähtsust.

Hariduskontekstis, eriti ülikoolides, on tudengite teadlikkus küberturvalisuse riskidest IoT-seadmete kasutamisel kriitilise tähtsusega. Uuringud näitavad, et paljud kasutajad ei ole piisavalt teadlikud nutiseadmetega seotud riskidest (Pew Research Center, 2019). Nende ohtude hulka kuuluvad andmepüük, viirused, volitamata juurdepääs isikuandmetele ja infolekked. Ülikoolide kontekstis, kus selliste seadmete kasutamine on tavaline, suurendavad riske turvamata WiFi-võrkude laialdane kasutamine ja aktiivne andmete jagamine üliõpilaste vahel. Turvaprobleemid tekivad sageli kasutajate teadmiste ja teadlikkuse puudumisest, muutes nad haavatavaks sotsiaalse inseneri ja muude pettustüüpide rünnakutele. Kasutajate käitumist mõjutavate tegurite mõistmine on võtmetähtsusega küberturvalisuse taseme

tõstmisel (Bada *et al.,* 2015; Wang *et al.,* 2021). Tudengid, õppejõud ja administratiivpersonal muutuvad nii sihtmärkideks kui ka potentsiaalseteks ohuallikateks (Lella, 2023).

Kõige olulisem on see, et hoolimata keerukate tehniliste kaitsemeetmete, näiteks viirusetõrje ja tulemüüride olemasolust, on infosüsteemide turvalisuse seisukohalt sageli määravaks teguriks lõppkasutajate käitumine ja tegevus (Bada *et al.,* 2015; Wang *et al.,* 2021). Näiteks võivad tõsiste turvarikkumisteni viia andmepüügi e-kirjade kriitikavaba käsitlemine, nõrkade või korduvkasutatavate paroolide hooletu kasutamine ja elementaarse digitaalse hügieeni eiramine (RIA, 2023).

Nutiseadmed mängivad kahekordset rolli küberturvalisuse valdkonnas. Ühelt poolt võivad nad parandada turvalisust läbi automatiseerimise ja efektiivsema andmete haldamise. Teiselt poolt loovad üha suurenev ühendatud seadmete arv uusi haavatavusi ja ründevektoreid küberruumi kurjategijate jaoks. Nutiseadmete mõistmine ja nende mõju igapäevaelule ja küberturvalisusele on võtmetähtsusega turvalisemate tehnoloogiate ja kaitsestrateegiate arendamisel. On oluline jätkata uurimistööd selles valdkonnas, et tuvastada potentsiaalsed riskid ja välja töötada tõhusad meetodid nende ohtude ennetamiseks ja reageerimiseks (Lella, 2023).

1.4 Teadlikkuse hindamine kõrghariduses

Tänapäeval täheldatakse maailma teadusringkondades uurimuste puudust, mis hindaksid üliõpilaste kompetentsust küberjulgeoleku valdkonnas (Zwilling *et al.,* 2020). Kõrghariduse kontekstis omandab veebipõhine õpe, mis on tingitud internetiressursside kättesaadavusest, olulist tähtsust haridussüsteemide tuleviku arengu jaoks (Harno, 2023). On oluline rõhutada, et interneti juurdepääs koos infotehnoloogiatega tagab üliõpilastele olulise paindlikkuse ja autonoomia (Meola, 2016). Seega mängib nende suhtumine ja taju küberjulgeolekusse olulist rolli isikliku kaitse tagamisel veebipõhiste ohtude eest. Täheldatakse inimeste kasvavat sõltuvust internetitehnoloogiatest igapäevastes ülesannetes, mis suurendab nende osalust küberseotud tegevustes. Efektiivsed kooliprogrammid tõestavad üliõpilaste loovmõtlemise ja kollektiivse probleemilahendamise oskuste arengut, mis hõlmab paindlikku ja kohandatavat lähenemist disainmõtlemise protsessile, kasutades arenenud IoT-tooteid ja -süsteeme (Tae, 2017).

Siiski esineb probleem põhiteadmiste puudulikkusest küberohtude ennetamisel. Samuti on märgitud, et põhiline teadlikkus küberjulgeolekust ei ole piisav küberohtude ja -riskide minimeerimiseks (Hossain, 2021). Abawajy (2012) poolt läbiviidud uuringud näitavad, et mobiiltelefonide kasutamisel küberjulgeolekuga seotud küsimusi uuritakse sageli tehnilisest vaatenurgast, samas kui inimfaktori tähtsust tehnoloogiatega suhtlemisel alahinnatakse (Abawajy, 2012).

Välisriikide uuringute raames läbi viidud küsitlus Ameerika Ühendriikides paljastas, et märkimisväärne osa ameeriklastest seisab silmitsi andmevargusega seotud probleemidega (Pew Research Center, 2017). See avastus viitab sügavale rahva umbusule erinevate institutsioonide, sealhulgas föderaalse valitsuse ja sotsiaalvõrgustike vastu, mis puudutab nende võimet tõhusalt kaitsta kodanike isikuandmeid. Lisaks näitab Pew Research (2017) keskuse poolt läbiviidud uuring, et paljud inimesed ei järgi oma isiklikus elus küberjulgeoleku põhimõtteid, mis hõlmab paroolide haldamise soovituste eiramist ja mobiilseadmete turvameetmete tähelepanuta jätmist. Need andmed rõhutavad kriitilist tähtsust tõsta üldsuse teadlikkust küberjulgeoleku tähtsusest ja vajadusest rakendada tõhusaid isikuandmete kaitse strateegiaid (Pew Research Center, 2017).

Seetõttu on väga oluline mõista, et kool on keskkond, kus luuakse praktiline alus tulevaseks suhtlemiseks nutiseadmetega, sealhulgas oskused nende kasutamiseks ja teadlikkus nende ohutusest (Kouroupis, 2023). Kuid kahjuks Tallinna Tehnikaülikoolis läbiviidud küberjulgeoleku ja digitaalse turvalisuse teemaline uurimus näitab, et koolidel on veel palju tööd teha küberjulgeoleku tagamisel (Raudla, 2019). Uuring rõhutab olulisi lünki digitaalsete oskuste õpetamisel ja isegi õpetajate kompetentsuses, kes peaksid edastama olulised turvalise kasutamise oskused. Seni on koolid käsitlenud digipädevuse õpetamist turvalisuse valdkonnas kui vabatahtlikku tegevust, ilma süstematiseeritud õppematerjalide loomiseta selle protsessi toetamiseks (Raudla, 2019).

Uuring, mis viidi läbi California ülikooli esmakursuslaste seas, näitas, et on levinud tendents mitte lugeda privaatsuspoliitika dokumente ja kasutustingimusi, kuid samal ajal jälgitakse teadlikult isikuandmetele juurdepääsu piiramist rakendustes turvalisuse kaalutlustel (Moallem, 2017). Teises uuringus Silicon Valley's selgus, et paljud tudengid ei mõista, et nende andmed võivad olla ohus isegi siis, kui nad on teadlikud pidevast oma tegevuse jälgimisest (Moallem, 2019). Küberohtude muutlikkus, nagu näiteks õngitsemine ja muud pettusmeetodid, nõuavad kohanduvate küberjulgeoleku programmide olulisust. See probleem leidis kinnitust ka Zwilling jt (2020) läbiviidud uuringus, mis keskendus küberjulgeolekualase

teadlikkuse, teadmiste ja kaitsevahendite kasutamise käitumise seoste analüüsimisele üldpopulatsioonis ja neljas riigis – Iisraelis, Sloveenias, Poolas ning Türgis. Uuringu tulemused näitasid, et kuigi internetikasutajad on teadlikud küberohtudest, rakendavad nad praktikas vaid minimaalseid kaitsemeetmeid (Zwilling *et al.*, 2020).

2021. aastal läbiviidud uurimus käsitles küberjulgeoleku teadlikkust, teadmisi ja käitumist Ungari ja Vietnami ülikooliõpilaste seas (Tick, 2021). Uuringus kasutati andmete kogumiseks küsimustikke, millele vastas 313 erinevate kursuste ja erialade tudengit. Andmete kvantitatiivse analüüsi jaoks rakendati SPSS programmi. Uuringu tulemused näitasid, et kõigil osalejatel on puudujäägid küberjulgeoleku alastes teadmistes, mis põhjustab madalat teadlikkust küberohtudest. See kehtib hoolimata kultuurilistest ja sotsiaalsetest erinevustest osalejate päritoluriikides (Tick, 2021).

Siiski ei oma mitte ainult õpilased, vaid ka õpetajad küberjulgeoleku valdkonnas nõrku teadmisi. Gallego-Arrufat jt (2019) uuringu põhijäreldused Hispaanias ja Portugalis tegutsevate eelkooliõpetajate seas näitavad, et nende digitaalse turvalisuse alane kompetentsustase on keskmine. Kuigi neil on turvalisuse suhtes hea suhtumine, jäävad turvalise ja vastutustundliku internetikasutuse teadmised ning oskused puudulikuks. Küsitluse, mis sisaldas 59 küsimust, tulemused näitasid, et 47% osalejatest seavad ohtu oma digitaalse turvalisuse, näiteks jagades ebasobivalt infot ja digitaalset sisu, kasutamata keerulisi paroole ning eirates digitaalse identiteedi ja maine mõisteid. See viitab vajadusele täiustada õpetajate koolitust turvalisuse, privaatsuse ja digitaalse identiteedi alal, mis on oluline osa esialgsest koolitusest ja nõuab edasisi uuringuid, et paremini ette valmistada digitaalselt kompetentsemaid kodanikke (Gallego-Arrufat *et al*., 2019).

Siiski on olemas uuringuid (Mason *et al*., 2023; Triplett, 2023), mis näitavad, et aktiivne uuenduslike õppemeetodite rakendamine õppeprotsessis parandab üldisi õpitulemusi. Näiteks hiljuti Inglismaal läbi viidud uuring Mason jt (2023) keskendus praktilise kaasamise ja mängustamise tõhususe uurimisele. Uuring hõlmas Avatud Ülikooli õppeplatvormi 'Küberjulgeoleku õppimise mängustatud kursus' efektiivsuse hindamist. Kasutati segameetodeid ja eel-järel eksperimentaalset disaini, milles osales 43 üliõpilast. Osalejad täitsid enne ja pärast kursust küsimustikke, mis käsitlesid informatsiooniturvalisuse aspekte. Tulemused näitasid, et üliõpilaste teadmistes, suhtumistes ja käitumises toimus märkimisväärne tõus, liikudes 'mõistlike' eelkoolitustasemete juurest 'väga kõrgetele' järelkoolitustasemetele. Uuring kinnitab, et mängulistel ja praktilistel õppemeetoditel on oluline mõju üliõpilaste teadlikkuse suurendamisele ja oskuste arendamisele, valmistades neid

tõhusalt ette tegelikeks küberohtudeks (Mason *et al*., 2023; Triplett, 2023). See tähendab, et praktilised küberjulgeoleku õppused osutuvad äärmiselt tõhusaks, pakkudes õpilastele realistlikku ja keerukat õpikeskkonda, mis on kriitilise tähtsusega meeskondlikuks õppeks eksperttasemel. Osalemine reaalsete küberstsenaariumide ümber struktureeritud simulatsioonides suurendab oluliselt küberjulgeoleku alaseid teadmisi, süvendab mõistmist ja aitab rakendada teoreetilisi teadmisi praktikas (Karjalainen jt, 2020). Uuringu raames Triplett (2023), mis keskendus õppekavades kasutatavate strateegiate uurimisele, pöörati erilist tähelepanu mängupõhiste meetodite kasutamisele õpilaste teadlikkuse tõstmiseks küberturvalisuse osas. Kümne uuringu analüüs näitas, et mänguline lähenemine võib oluliselt suurendada õpilaste huvi küberturvalisuse valdkonna ametite vastu (Triplett, 2023). Mängud, mis simuleerivad nii kaitse- kui ründesituatsioone, aitavad õpilastel paremini mõista, kuidas vastu seista küberturvalisuse ohtudele ja arendada vastavaid oskusi (Triplett, 2023; Zaharakis *et al.,* 2016).

Uuringud (Silva, 2023; Triplett, 2023) kinnitasid, et sellised strateegiad tõstavad mitte ainult õpilaste teadmiste taset, vaid motiveerivad neid valima karjääri küberturvalisuse valdkonnas. See on eriti oluline arvestades ülemaailmset kvalifitseeritud spetsialistide puudust selles sektoris. Mängupõhised meetodid osutusid tõhusaks õpilaste tähelepanu köitmiseks ja nende soovi äratamiseks saada küberturvalisuse professionaalideks (Triplett, 2023).

Tõhusa turvalisuse teadlikkuse programmi väljatöötamine ja rakendamine on küberjulgeoleku tugevdamise võtmetähtsusega etapp. Alqahtani (2022) hiljutise uuringu peamine eesmärk oli hinnata üliõpilaste teadlikkuse taset kolme kriitiliselt tähtsa aspekti osas: paroolide turvalisus, brauserite turvalisus ja sotsiaalmeedia kasutamine. Uuringu tulemused näitasid, et teadmised nendes valdkondades avaldavad olulist mõju üliõpilaste üldisele küberjulgeolekuteadlikkusele. Üliõpilased mõistsid küberjulgeolekuteadlikkuse tähtsust, mis on kriitilise tähtsusega nende isikliku ja professionaalse turvalisuse tagamiseks digitaalses maailmas (Alqahtani, 2022).

Pencheva jt (2020) uuring toob esile, et küberturvalisuse integreerimine keskharidusse on keeruline, kuna õpilastel puudub arusaam karjäärivõimalustest ja internetis turvaliselt käitumisest, samas kui õpetajatel napib vajalikke teadmisi ja ressursse. Kolme ühepäevase õpetajate töötoa põhjal tuvastati takistused ja võimalused küberturvalisuse õpetamiseks keskkoolides. Leiti, et kuigi õpilased on oma õpetajatest teadlikumad küberturvalisusest, ei

mõista nad siiski karjäärivõimalusi ega kuidas internetis turvaliselt käituda. Õpetajate puhul on peamiseks probleemiks asjakohaste teadmiste ja õppematerjalide puudumine.

Eesti koolisüsteemide ja haridusasutuste kontekstis näitab statistika analüüs, et 2021. aastal said koolid ja haridussüsteemid sageli küber-rünnakute sihtmärgiks. Sellised rünnakud võivad olla eriti hävitavad, kuna need segavad haridusprotsessi ja seavad ohtu õpilaste ning õpetajate isikuandmete konfidentsiaalsuse. Näiteks 2022. aastal selliste rünnakute arv vähenes, mis osaliselt võib viidata küberjulgeoleku taseme tõusule haridusasutustes või ründajate taktika ajutisele muutumisele (RIA, 2022).

2. METOODIKA

Käesolev uurimistöö peatükk on pühendatud kvantitatiivse uurimuse metoodikale, mis on suunatud Eesti ülikoolide esmakursuslaste digitaalse teadlikkuse taseme hindamisele küberjulgeoleku valdkonnas. Tuginedes digipädevuse programmile DigComp (2022), analüüsib uurimus, kui tõhusalt haridussüsteem valmistab noori ette toime tulema küberjulgeoleku riskidega, arvestades nutiseadmete laialdast kasutust.

Peatüki peamised teemad hõlmavad valimi kirjeldust, andmekogumismeetodeid ja andmeanalüüsi lähenemisviise. Erilist tähelepanu pööratakse metoodilisele lähenemisele, mis tagab saadud tulemuste usaldusväärsuse ja kehtivuse, võimaldades teha põhjendatud järeldusi sihtrühma digipädevuse kohta.

Lisas (Lisa A) on esitatud välja töötatud küsimustik, mis sisaldab küsimusi, katvaid erinevaid digipädevuse aspekte küberjulgeoleku kontekstis. Küsimustik on mõeldud hindama nii üliõpilaste üldist digitaalse teadlikkuse taset kui ka nende spetsiifilisi teadmisi ja oskusi, mis on seotud digitehnoloogiate ja nutiseadmete kasutamisega.

Uuringu küsitlus viidi läbi kahe kuu jooksul, märtsist aprillini. Selleks ajaks olid kirjad saadetud 7 Eesti kõrgkooli spetsialistidele, kes tegelevad õppekorralduse ja õppejõududega, palvega levitada kutset osalema uuringus esmakursuslaste seas koos lingiga osalemiseks.

2.1 Uurimisküsimused

Uurimisküsimused ja hüpoteesid töötati välja, lähtudes Euroopa Komisjoni digipädevuse raamistikust kodanikele (Vuorikari *et al.*, 2022). See dokument pakub süstemaatilist lähenemist digipädevuse mõõtmisele ja arendamisele, hõlmates erinevaid oskusi ja teadmisi, mis on vajalikud edukaks toimetulekuks digitaalses ühiskonnas (Vuorikari *et al.*, 2022). Eesmärk oli luua struktureeritud küsimustik, mis võimaldab hinnata Eesti ülikoolide esmakursuslaste digipädevuse taset, erilise rõhuasetusega teadlikkusel küberjulgeoleku valdkonnas ja suhtumisel sellesse. Suurim rõhk asetati kõige aktuaalsematele probleemidele, lähtudes riigis kõige värskematest andmetest.

Lisaks sellele põhines uurimus ka eelnevalt läbiviidud uurimustööl küberjulgeoleku ja küber teadlikkuse valdkonnas kooliõpilaste seas, mis koosnes kolmest põhietapist: küberjulgeoleku alase käitumise ja suhtumise hindamine kasutades enesediagnostika põhimõtteid (Antunes, 2021). Lisaks kasutati kogemust küsitluse kohandamisel, mis oli loodud hindamaks teadlikkust, suhtumist, käitumist ja uskumusi küberjulgeoleku valdkonnas kolledži üliõpilaste seas (Schaffer & Debb, 2019). Selles lähenemisviisis suurendati küsimuste arvu küsitluses 30-ni, mis võimaldas üksikasjalikumalt uurida ja analüüsida neid aspekte õpilaste seas.

Uuringus küsitluse loomiseks küberjulgeoleku teadlikkuse taseme hindamiseks kasutati ka kvalifikatsiooni süsteemset hindamise lähenemist (Tempestini *et al.,* 2023). See lähenemine avas võimalused õppeprogrammide potentsiaali integreerimiseks, võimaldades analüüsida ja võrrelda kooliõpilaste kogemusi küberjulgeoleku valdkonnas ning pakkudes väärtuslikku teavet ülikooli esmakursuslaste digipädevuse uurimiseks. See lähenemine võimaldas integreerida ja võrrelda kooliõpilaste kogemusi küberjulgeoleku valdkonnas, pakkudes väärtuslikku taustateavet ja konteksti ülikooli esmakursuslaste digipädevuse uurimiseks.

Uurimisküsimused:

- Küberjulgeolekuks valmisoleku hindamine: Kuidas Eesti ülikoolide esmakursuslased mõistavad digikeskkonna küberjulgeoleku põhimõtteid ja riske?
- Üliõpilaste suhtumine küberjulgeolekusse: Kuidas suhtuvad valitud Eesti ülikoolide esmakursuslased küberjulgeoleku tähtsusesse ja oma rolli selles?

Ankeedi koostamisel võeti arvesse viit peamist kompetentsivaldkonda, määratletud DigComp raames: info- ja andmelugemisoskus, kommunikatsioon ja koostöö, digitaalse sisu loomine, turvalisus ja probleemide lahendamine (Vuorikari *et al.*, 2022). Iga valdkond hõlmab spetsiifilisi kompetentse, mis võimaldavad hinnata ja arendada üliõpilaste digioskusi. Ankeet on kujundatud nii, et saada ülevaade nii üldisest digipädevuse tasemest kui ka konkreetsematest oskustest, mis on olulised küberjulgeoleku kontekstis nutiseadmete kasutamisel (Antunes, 2021). Küsimuste koostamiseks tehti lisaks põhjalik ülevaade teemakohasest kirjandusest ja uurimustöödest, mis keskenduvad mõistete, terminite ja funktsioonide määratlemisele. Sellise kirjanduse hulka kuulusid peamiselt akadeemilised artiklid ja juhendid, mis käsitlesid digitaalset identiteeti, autentimismeetodeid ja andmekaitse parimaid taktikaid (Antunes, 2021; Harno, 2023; Kanellos, 2020; PRAXIS, 2017; Vuorikari *et al.*, 2022)

See lähenemisviis on suunatud praeguse olukorra hindamisele ning potentsiaalsete lünkade ja vajaduste tuvastamisele digipädevuse arendamisel, eriti küberjulgeoleku riskide mõistmisel ja haldamisel. Lisas „A“ esitatud küsimustik sisaldab küsimusi, suunatud küberjulgeoleku, digitehnoloogiate abil koostöö ja kommunikatsiooni ning digikeskkonnas tekkivate tehniliste probleemide lahendamise oskuste hindamisele. Küsimustik on loodud selleks, et koguda andmeid selle kohta, kui hästi on üliõpilased digitaalse turvalisusega kursis, kuidas nad saavad oma seadmeid ja andmeid kaitsta ning millised oskused neil on digitehnoloogiate kasutamisel tekkivate probleemide lahendamiseks.

Küsimused olid koostatud arvestades, et vastamine on anonüümne ning andmeid kasutatakse ainult käesolevas magistritöös. Kõik uuringus osalejad olid eelnevalt kahekordselt teavitatud anonüümsuse tagamise ja andmete kasutamise tingimustest: esmalt kutse saatmisel osalema uuringus ja seejärel uuringu veebilehel. Osalejate nimed, sugu ega muud isiklikud andmed ei kogutud.

Algne küsitlus viidi läbi kolme testversiooni kaudu, kus Tartu Ülikooli esmakursuslased osalesid juhusliku valiku alusel. Pärast küsitlusele vastamist viidi läbi lühikesed intervjuud, et saada tagasisidet, soovitusi ning võimaldada vastajatel jagada oma muljeid küsitluse läbimisest. See samm võimaldas täiendada ja parandada küsitlust ning kinnitada küsimuste asjakohasust ja arusaadavust, tagades, et järgnevas uuringus kogutud andmed oleksid usaldusväärsed ja tähendusrikkad.

Testi ajal selgus, et keskmine küsimustiku täitmise aeg ei ületanud 9 minutit, mis näitas küsimustiku optimaalset pikkust ja keerukust. Kõige mugavamaks täitmisvormiks osutus Microsoft Forms, mille kasutajasõbralikkus ja paindlikkus olid eriti hinnatud. Otsustati laiendada küsitluse sihtrühma ja luua ingliskeelne versioon. Microsoft Forms'i funktsionaalsus võimaldas integreerida vormi keelevaliku võimaluse, andes vastajatele võimaluse valida eesti ja inglise keele vahel. Lisaks lisati paljudele vastusevariantidele võimalus sisestada oma vastusevariant, juhul kui leitud variantide hulgas ei olnud sobivat. See samm parandas oluliselt küsitluse kättesaadavust ja paindlikkust, võimaldades koguda laiemat ja mitmekesisemat tagasisidet.

Aktiivse levitamise ja küsimuste esitamise perioodil lisati samuti kõige sagedamini esitatud vastusevariantid, mida küsitluses osalejad isiklikult lisasid, peamiste vastusevariantide hulka. See tagas parema integratsiooni ja kiirendas suhtlust, võimaldades tulevastel vastajatel valida laiemast vastuste spektrist, mis peegeldas üldisi suundumusi ja eelistusi. Selline lähenemine lihtsustas andmekogumise protsessi ja rikastas lõppanalüüsi, tänu täpsemale osalejate arvamuste kajastamisele.

2.2 Valim

Valim moodustati, kasutades sihtgrupina olemasolevaid tudengeid ja rakendades mittetõenäosuslikku lähenemist (Õunapuu, 2014). See valik oli tingitud uurimistöö piiratud ajalisest ja ressursilisest raamistikust ning soovist viia andmekogumine läbi võimalikult efektiivselt. Kuigi selline lähenemine ei võimalda tagada osalejate võrdset valikuvõimalust üldpopulatsioonist, võimaldab see siiski kasutada laia ja mitmekesist andmekogumit, mis on saadud otse sihtgrupilt. Eesti ülikoolide esmakursuslaste seas küsitluste levitamine tagas andmebaasi laiuse ja mitmekesisuse, aidates süvendatult mõista praegust olukorda ja vajadusi seoses digipädevuse ning küberjulgeolekuga.

Ülikoolide valimi koostamisel kasutati Eesti Hariduse Infosüsteemi (EHIS, 2024) andmeid, mis võimaldasid hõlmata laia spektrit ülikoolikursusi ja tagada valimi ajakohasus ning täielikkus. Küsitluste levitamine kõigis Eesti ülikoolide esmakursuslaste seas võimaldas koguda vastuseid, mis on aluseks põhjalikule analüüsile noorte digipädevuse ja küberjulgeoleku alase teadlikkuse praegusest tasemest.

2.3 Andmete kogumine ja analüüsimeetodid

2024. aasta andmete põhjal EHIS.ee kodulehel on Eestis 7 ülikooli: Tallinna Ülikool, Estonian Business School, Eesti Muusika- ja Teatriakadeemia, Tartu Ülikool, Tallinna Tehnikaülikool, Eesti Maaülikool ja Eesti Kunstiakadeemia. Andmekogumiseks esmakursuslaste seas loodi veebipõhine küsimustik, millele ülikoolide õppekorralduse ja -juhtimise spetsialistid said juurdepääsu. Koostöös akadeemilise juhendajaga valmistati ette kutsekiri, milles paluti esmakursuslastel küsitluses osaleda, rõhutades osalemise tähtsust ja vastuste täielikku konfidentsiaalsust.

Andmekogumise protsessis kasutati Eesti eri ülikoolide tudengite seas läbiviidud veebiküsitlust. Küsitlus viidi läbi kasutades nii Microsoft Forms kui ka Google Forms platvorme, tagades andmekogumise protsessi mugavuse ja kättesaadavuse. Küsitluse disain sisaldas struktureeritud küsimusi, mis olid hoolikalt koostatud vastavalt uurimiseesmärkidele, põhinedes DigComp raamistikul (Vuorikari *et al.*, 2022). Selline kvantitatiivne uurimismeetod, kombineeritud andmete statistilise analüüsiga, tagas saadud tulemuste objektiivsuse ja täpsuse (Õunapuu, 2014). Lisaks võimaldas valitud mittetõenäosuslik valimimeetod uurimistööd läbi viia efektiivselt ja operatiivselt, arvestades projekti piiratud ressursse.

Andmekogumine algas märtsis ja lõppes aprilli lõpus 2024. aastal. Uuringus osales kokku 73 inimest. Tagasiside põhjal õppekorralduse spetsialistidelt selgus, et kutse osaleda küsitluses õnnestus levitada kõigi esmakursuslaste seas ainult Eesti Maaülikoolis, Tallinna Ülikoolis ja Tartu Ülikoolis. See teave aitab mõista andmekogumise protsessi ulatust ja potentsiaalseid piiranguid uuringu valimis.

Kogutud andmete analüüs viidi läbi kasutades kvantitatiivseid analüüsimeetodeid, mis võimaldas teostada põhjaliku analüüsi üliõpilaste digipädevuse tasemest ja teadlikkusest küberjulgeoleku osas. Peamised analüüsimeetodid hõlmasid kirjeldavat statistikat, korrelatsioonianalüüsi ja regressioonianalüüsi, mis võimaldasid hinnata erinevate digipädevuse aspektide ja küberjulgeolekualase teadlikkuse taseme vahelisi seoseid (Õunapuu, 2014).

Uuringus uuriti erinevate digipädevuse taseme ja küberjulgeoleku teadlikkuse omavahelisi seoseid üliõpilaste seas. Regressioonianalüüsi kasutati digipädevuse aspektide ja küberjulgeoleku teadlikkuse taseme vaheliste seoste hindamiseks. Põhifookus oli sellistel

tunnustel nagu internetis veedetud aeg, haridustase ja küberjulgeolekualase ettevalmistuse tajumine.

Uuringu tulemuste usaldusväärsuse ja kehtivuse tagamiseks kasutati andmete potentsiaalsete moonutuste analüüsi. Peamine rõhk oli regressioonianalüüsil, mis hõlmas oluliste muutujate, nagu vanus, haridustase ja internetis veedetud aeg, mõju hindamist osalejate küberjulgeoleku tajumisele (Õunapuu, 2014). See analüüs võimaldas hinnata, kuidas iga tegur mõjutab vastuste varieeruvust ja aitas tuvastada andmetes struktuurilisi moonutusi, mis omakorda aitasid täpsustada ja kohandada uuringu lõpptulemusi.

3. TULEMUSED

Käesolevas peatükis esitatakse põhjalik ülevaade küberjulgeoleku alase teadlikkuse ja hoiakute uurimusest, mis õnnestus läbi viia Tallinna Ülikoolis, Tartu Ülikoolis ning Eesti Maaülikoolis, hoolimata sellest, et kutseid saadeti laiali kõikidele Eesti ülikoolidele. Uurimus keskendub tudengite internetikasutuse põhiaspektidele, sealhulgas sellele, kui palju aega nad keskmiselt veebis veedavad ning millistele tegevustele nad internetis enim aega pühendavad. Samuti analüüsitakse osalevate tudengite haridustaset ja erialade valikut, erilist tähelepanu pöörates tehnilise suunitlusega erialade üliõpilastele. Selline lähenemine võimaldab tuvastada üldisi suundumusi ja mõista, kuidas erinevad erialad võivad mõjutada tudengite küberjulgeoleku alaseid teadmisi ja hoiakuid.

Teises peatükis keskendutakse empiirilistele tulemustele, sealhulgas erinevate tegurite, nagu internetis veedetud aeg ja küberjulgeoleku alane ettevalmistus, vahelise korrelatsioonianalüüsi tulemustele. Vaadeldakse küberjulgeolekuga seotud riskide tajumise ja käitumise erinevusi. Samuti arutatakse teemasid ja valdkondi küberjulgeolekus, millele tudengid leiavad, et õppeprogrammides tuleks rohkem tähelepanu pöörata.

Kolmandas peatükis analüüsitakse seoseid internetis veedetud aja, haridustaseme ja küberjulgeoleku alase ettevalmistuse tajumise vahel. Tulemused näitavad, et mida rohkem tudengid internetis aega veedavad, seda vähem tunnevad nad end küberjulgeoleku valdkonnas ettevalmistatuna. Samuti leiti nõrk positiivne seos haridustaseme ja küberjulgeoleku teadmiste vahel, mis rõhutab tehniliste erialade tudengite paremat ettevalmistust võrreldes humanitaarerialadega.

3.1 Tudengite teadlikkuse taseme hindamine ja empiirilised tulemused

Uuring hõlmas 87 kolme Eesti ülikooli esmakursuslast, kes jagasid oma vaateid ja teadlikkust küberjulgeolekust. Osalejate keskmine vanus oli 22 aastat, vanusevahemikuga 19 kuni 44 aastat, mis rõhutab valimi nooruslikku suunitlust. Enamus tudengitest (41.1% ehk 38 osalejat) veedavad internetis üle 6 tunni päevas, peegeldades nende kõrgetasemelist kaasatust veebitegevustesse. Umbes 34.2% (31 osalejat) veedavad veebis 4-6 tundi päevas ja 20.5% (15 osalejat) 2-4 tundi. Vaid väike osa, 3.4% (3 osalejat), märkis, et veedab internetis vähem kui ühe tunni päevas.

Haridustaseme järgi oli enamus vastajatest (65 87-st ehk 74.71%) omandanud gümnaasiumihariduse, 14 osalejat (16.09%) olid õppinud kutsekoolis ja 8 vastajat (9.20%), kes juba omasid kõrgharidust, õppisid kõrgkoolis esimesel kursusel.

Eriala valikutes domineerisid inseneriteadused, kus 59.77% (52 osalejat) spetsialiseeruvad sellele valdkonnale, järgnesid loodus- ja täppisteadused 24.14% (21 osalejat). Ülejäänud jaotuvad erialade vahel, nagu meditsiin, õigusteadus, aiandus, keskkonnakaitse, kunst, bioloogia ning keeled ja kirjandus.

Uuring küberturvalisuse tõstmise eelistustest näitas, et enamik, 51.7% (45 üliõpilast), peavad teadlikkuse suurendamist ja koolitust peamisteks vahenditeks infotehnoloogia süsteemide kaitse tugevdamisel. 17.2% (15 üliõpilast) pidasid kriitiliselt oluliseks tarkvara ja paroolide regulaarset uuendamist ning turvameetmete kasutamist, sealhulgas viirusetõrjeid ja tulemüüre. Väikseim protsent, 3.4% (3 üliõpilast), märkis tootjate vastutust toodete turvalisuse eest.

Valiku osas kindluse puudumine, mida väljendas 10.3% (9 üliõpilast), tõstatab küsimuse vajadusest süvendada teadmisi selles valdkonnas. Need tulemused viitavad vajadusele läheneda küberturvalisusele kompleksselt, ühendades hariduslikud, tehnilised ja regulatiivsed aspektid.

Tabel 1: *Internetis veedetud aja jaotus*

Internetis veedetud aeg	Vastanute arv	Protsent koguarvust
Üle 6 tunni	38	41.1%
4-6 tundi	31	34.2%
2-4 tundi	15	20.5%
Alla 1 tunni	3	4.1%

Tabel 2: *Vastanute haridustase*

Haridustase	Vastanute arv	Protsent koguarvust
Gümnaasium	65	74.71%
Kutsekool	14	16.09%
Kõrgharidus/ülikool	8	9.20%

Tabel 3: *Küberturvalisusega seotud ettevalmistuse tajumine*

Ettevalmistuse tajumine	Vastanute arv	Protsent koguarvust
Neutraalne	53	60.9%
Ei nõustu	25	28.7%
Nõustun	9	10.3%

Tabel 4: *Eelistatud meetmed küberturvalisuse tõstmiseks*

Küberturvalisuse tõstmise meetmed	Vastanute arv	Protsent koguarvust
Teadlikkuse suurendamine ja koolitused	45	51.7%
Tarkvara ja paroolide regulaarne uuendamine	15	17.2%
Tehnilised kaitsevahendid (viirusetõrje ja tulemüürid)	15	17.2%
Ei ole kindel / Raske öelda	9	10.3%
Tootjate vastutus (seadmete ja tarkvara tootjad peaksid tagama küberturvalisuse)	3	3.4%

3.2 Riskide tajumise ja kasutamise erinevused

Selle uurimuse raames tuvastati mitmeid korrelatsioone, mis viitavad seostele internetis veedetud aja, haridustaseme ja küberjulgeoleku alase ettevalmistuse tajumise vahel. Siiski tuleb märkida, et analüüsiti ainult korrelatsiooni ja see ei tõesta põhjuslikke seoseid. Leiti, et on olemas negatiivne korrelatsioon (r=-0.62) internetis veedetud aja ja küberjulgeoleku alase ettevalmistuse tajumise vahel, mis võib osutada sellele, et suurem internetikasutus ei pruugi kaasa tuua paremat valmisolekut küberjulgeoleku väljakutseteks. See võib viidata võimalikele puudujääkidele õppekavades, eriti aktiivsete internetikasutajate seas, kuid tulemuste piiratuse tõttu väikese valimi ja puuduvate eksperimentaalsete või eel- ja järeltestide tõttu ei saa teha kindlaid järeldusi põhjuslikkuse kohta.

Samuti tuvastati nõrk positiivne korrelatsioon (r=0.30) haridustaseme ja küberjulgeoleku alase ettevalmistuse tajumise vahel. See näitab, et tudengid, kellel on kõrgem haridustase, tajuvad end küberjulgeoleku valdkonnas paremini ettevalmistatuna. Siiski, jällegi, tuleb rõhutada, et tegemist on vaid tajutava ettevalmistusega ja see ei pruugi täielikult kajastada tegelikku oskuste taset.

Tulemuste usaldusväärsuse ja kehtivuse tagamiseks uuriti seoseid internetis veedetud aja, haridustaseme ja õpilaste küberturvalisuse alase valmisoleku tajumise vahel. Välja töötatud lineaarne regressioonimudel hõlmas kahte sõltumatut muutujat: internetis veedetud aeg ja haridustase. Sõltuvaks muutujaks oli küberturvalisuse valmisoleku tajumine. Regressioonianalüüsi tulemused näitasid, et keskmine ruutviga (MSE) on 0,31, mis viitab sellele, et mudeli ennustuste keskmine viga on umbes 0,31 sõltuva muutuja mõõtühikutes. See suhteliselt madal väärtus näitab mudeli adekvaatsust. Määramisväärtus (R^2) on 0,42, mis tähendab, et umbes 42% küberturvalisuse ettevalmistuse tajumise varieeruvusest võib seletada mudeliga, mis hõlmab internetis veedetud aega ja haridustaset. See üsna oluline tulemus rõhutab valitud ennustajate asjakohasust. Regressioonianalüüs näitas olulist mõju internetis veedetud ajal küberturvalisuse ettevalmistuse tajumisele. Haridustase mõjutab ka, kuid vähemal määral. Siiski nõuavad need andmed täiendavat uurimist, eelistatavalt kasutades kontrollgruppe, et paremini mõista seoseid ja võimalikke kausaalseid seoseid.

Uuringust selgus ka, et humanitaar- ja sotsiaalteaduste tudengid tajuvad madalamat teadlikkust küberjulgeolekust võrreldes tehniliste erialade tudengitega. See rõhutab

interdistsiplinaarse lähenemise olulisust küberjulgeoleku õpetamisel, et kõik erialad oleksid kaasatud ja informeeritud.

Uuringus osalejate hinnangud oma kooli õppekavale näitasid, et arvamused on jagunenud. Umbes osalejatest suhtusid neutraalselt, samas kui väljendasid selget rahulolematust. Küberturvalisuse ettevalmistuse kohta küsimustele vastates selgus, et 60,9% osalejatest suhtuvad neutraalselt oma õppekava ettevalmistusse. Umbes 28,7% väljendasid selget nõusoleku puudumist, rõhutades vajadust haridusstandardite parandamiseks. Eriti tähelepanu vajavad valdkonnad olid andmepüük ja sotsiaalne inseneria (43 mainimist 87-st), isikuandmete kaitse sotsiaalvõrgustikes (22 mainimist) ja turvalised internetimaksed (10 mainimist). Viimased 12 kirjutasid, et kõik nimetatud suunad vajavad uurimist, märkides samas, et nende ülikooli õppekavas puudub küberturvalisuse aine täielikult, mis rõhutab vajadust käsitleda küberturvalisuse õpetust terviklikult.

See viitab vajadusele täiustada haridusstandardeid ja integreerida küberjulgeoleku alane õpe tõhusamalt kõigisse õppekavadesse. Eeltoodu põhjal on oluline jätkata uurimistööd suuremate ja mitmekesisemate valimitega ning kasutada eksperimentaalseid lähenemisi, mis võimaldaksid paremini mõista ja kinnitada leitud seoseid.

4. ARUTELU JA JÄRELDUSED

Käesolevas peatükis esitatakse uuringu tulemused, mis keskenduvad digitaalse kirjaoskuse ja küberjulgeoleku teadlikkuse hindamisele Eesti ülikoolide esmakursuslaste seas. Peamine avastus oli lõhe tuvastamine tudengite aktiivse internetikasutuse ja nende küberohtudega toimetulekuks vajaliku ettevalmistuse puudulikkuse vahel. Enamik vastajaid veedab võrgus üle 6 tunni päevas, kuid arvab, et nende õppeprogrammid ei valmista neid piisavalt ette kaasaegsete küberohtude jaoks. Soovitused on esitatud nii tudengitele kui ka haridusasutustele. Vaatamata tulemuste olulisusele tuleb arvestada uuringu piiranguid, nagu fookus esmakursuslastele ja valimi piiratud maht.

On tähtis märkida, et kuigi käesolev uuring tuvastab erinevate tegurite vahelisi statistilisi seoseid, ei võimalda see tulemused kinnitada põhjuslikke suhteid nende vahel. Uuringu käigus ilmnesid mõned piirangud, mis mõjutavad järelduste kindlust. Väikese valimi suurus ja eksperimentaalsete sekkumiste puudumine piiravad võimalust teha kindlaid järeldusi põhjuslike seoste kohta. Sellised piirangud vähendavad uuringu tulemuste üldistatavust. Seetõttu on vajalik läbi viia täiendavad uuringud, et kinnitada või ümber lükata tuvastatud korrelatsioonid.

Tulevikus on vajalikud laiemad uuringud, et hinnata uuendatud õppeprogrammide mõju tudengite ettevalmistuse tasemele. Kokkuvõttes rõhutab uuring vajadust kohandada õppeprogramme digiajastu nõudmistele ja lisada neisse küberjulgeoleku õpetuse terviklik lähenemine.

4.1 Peamised leiud ja nende tõlgendus

Uuringu kõige olulisemaks tulemuseks oli ilmse lõhe avastamine tudengite kõrge internetitegevustesse kaasatuse ja nende tajutava küberjulgeolekuriskideks ettevalmistuse puudulikkuse vahel. See väljendus selles, et enamik küsitletuid veedab internetis üle 6 tunni päevas, kuid samal ajal väljendavad paljud neist neutraalset või isegi negatiivset arvamust oma õppeprogrammide küberohtude ettevalmistuse kohta. Seda täheldust kinnitavad ka teiste uuringute andmed, mis samuti rõhutavad kasvavat vajadust õppekavade järele, mis käsitleksid reaalseid küberohte (Corradini, 2020).

Kuigi vahendid mängivad olulist rolli teadlikkuse tõstmisel, peaksid need olema osa keerukamast ja mitmekülgsemast programmist, mille eesmärk on stimuleerida inimesi oma digitaalses keskkonnas käitumist muutma.

Uuring näitas, et üliõpilased, kellel on kõrgem haridustase, tunnevad end küberjulgeoleku valdkonnas paremini ettevalmistatuna. See viitab sellele, et kõrgema haridusega üliõpilastel võib olla suurem enesekindlus ja arusaam küberjulgeoleku küsimustest. Siiski on oluline märkida, et nende enesetaju ei pruugi alati täielikult kajastada nende tegelikke oskusi ja pädevusi selles valdkonnas. Selliseid järeldusi toetavad uuringud, mis näitavad, et haridus mängib olulist rolli üliõpilaste teadmiste ja arusaamade kujunemisel küberjulgeoleku küsimustes. Faktorid nagu tõsiduse tajumine, eakaaslaste käitumine ja teadlikkus küberohtudest varieeruvad oluliselt sõltuvalt vanusest ja haridustasemest (Alharbi & Tassaddiq, 2021). Küberjulgeoleku põhikursus, mis sisaldab praktilisi harjutusi, võib oluliselt parandada üliõpilaste teadmisi ja käitumist selles valdkonnas. Teadmised ja aktiivsus avaldavad märkimisväärset mõju üliõpilaste teadlikkusele küberjulgeoleku osas, mis rõhutab selliste õppekavade tähtsust üldise mõistmise ja digitaalkeskkonna turvalisuse edendamisel (Alqahtani, 2022).

Võrreldes varasemate uuringutega, näitab see, et kuigi noorte teadlikkus küberjulgeolekust suureneb, on märkimisväärne lõhe teadmiste ja oskuste vahel, mida nad omandavad, ja nende vahel, mis on vajalikud digikeskkonnas kaitsmiseks (Zwilling *et al.,* 2020). Seega rõhutab käesolev uuring kriitilist vajadust õppekavade kohandamiseks muutuva digitaalse maastikuga, kaasates aktuaalseid teemasid nagu andmepüük, sotsiaalne inseneeria, isikuandmete kaitse sotsiaalvõrgustikes. Siiski on see vaid osa vajalikest meetmetest.

4.2 Soovitused tudengitele ja õppeasutustele

Küberjulgeolekukultuuri tugevdamine on keeruline ülesanne, mis hõlmab tehnilisi, organisatsioonilisi ja inimfaktoreid. Selleks, et efektiivselt seista vastu küberohtudele, on vajalik rakendada terviklikku lähenemisviisi, mis arvestab mitte ainult tehnilisi lahendusi, vaid ka kultuurilist ja hariduslikku arengut. Uuringute kohaselt kaasaegne lähenemine rõhutab küberjulgeolekukultuuri kriitilist tähtsust, mis aitab vähendada küberrünnakute riske ning tugevdada nii organisatsioonide kui ka haridusasutuste vastupanuvõimet (Silva, 2023).

Hariduse roll on siin määrava tähtsusega. Erinevate haridusvormide – formaalsest kuni informaalsete ja mitteformaalsete meetoditeni – kaasamine on oluline küberjulgeolekut puudutavate teadmiste levitamisel ning teadlikkuse tõstmisel. Õppekavad, mis suurendavad teadlikkust küberjulgeolekust, aitavad kujundada positiivset kultuuri, mis on hädavajalik küberrünnakute ärahoidmiseks (Nasir, 2023). Uuringud näitavad, et süsteemne ja järjepidev teadlikkuse tõstmise programm, mis sisaldab nii teoreetilist õpet kui ka praktilisi treeninguid, on oluline, et ette valmistada õpilasi ja töötajaid reaalseteks küberohtudeks (Silva, 2023). Just selles aspektis peitub vajadus luua adekvaatseid õppekavasid, mis on suunatud teadlikkuse tõstmisele, õpetamisele ja hariduse andmisele küberjulgeoleku valdkonnas. Need kolm komponenti mängivad võtmerolli vastutustundliku käitumise kujundamises võrgukasutajate seas (Corradini, 2020).

Seega, küberjulgeolekukultuuri tugevdamiseks ja teadlikkuse arendamiseks on vajalik koolituse ja kvalifikatsiooni tõstmise integreerimine organisatsiooniliste muutustega ning iga protsessi osaleja isikliku kaasatusega, kuna küberjulgeolekukultuuri efektiivsus sõltub suuresti osalejate aktiivsest osalusest ja pühendumusest (Corradini, 2020).

Küberjulgeolekukultuur peab olema globaalne, kuna küberohtude mõju on piirideülene. Investeeringud haridusalgatustesse, mis tõstavad teadlikkust ja parandavad käitumist kübermaailmas, nõuavad olulist panust nii rahvusvahelistelt valitsusvälistelt organisatsioonidelt kui ka valitsusorganisatsioonidelt. Selline üleilmne koostöö aitab tagada, et küberjulgeoleku standardid ja praktikad on ühtlustatud ning piisavalt tugevad, et vastata kiiresti muutuvatele ohtudele (Pătrașcu, 2019).

Lisaks on vajalik pidev enesehindamine. Organisatsioonid ja haridusasutused peaksid regulaarselt hindama oma turvakultuuri küpsust, et mõista praegust olukorda ja tuvastada vajadused. See võimaldab neil arendada ja rakendada turvalisuse teavitamise programme, mis on kohandatud nende spetsiifilistele vajadustele (Corradini, 2020). Turvalise keskkonna kujundamise põhimõtetel põhinevalt on küberjulgeolekukultuuri loomise püüdluses esmatähtis ülesanne hinnangufaas — sisemine enesehindamine praeguse turvakultuuri küpsuse taseme määramiseks (Corradini, 2020). Praeguse olukorra ja probleemide mõistmine enesehindamise kaudu võimaldab tuvastada tegelikke vajadusi ja vältida turvalisuse teavitamise programmide väljatöötamist ja rakendamist, mis ei vasta nendele vajadustele.

See on otseselt seotud käitumise muutuse saavutamise ja kriitilise mõtlemise arendamisega, mis on aeganõudev protsess ja nõuab sügavat arusaamist inimloomusest ning

käitumismehhanismidest. Samuti on oluline mõista, et küberjulgeoleku strateegiate väljatöötamisel võivad füüsilisest maailmast pärit turvaharjumused pakkuda väärtuslikku inspiratsiooni (Corradini, 2020).

Käesolev uuring Eesti ülikoolides, mis hindab teadlikkust ja suhtumist küberjulgeolekusse, rõhutab, et küberjulgeolekukultuuri areng saab alguse praeguse olukorra ja probleemide põhjalikust mõistmisest läbi enesehindamise. Samuti rõhutatakse varasemates töödes olemasolevate õppekavade hindamise vajadust ja lünkade tuvastamist praegustes õppemeetodites. See etapp on kriitilise tähtsusega, kuna see loob aluse uute strateegiate juurutamiseks haridusasutustes.

Uute strateegiate olulisus seisneb nende võimes kohaneda kiiresti muutuva digitaalse maastikuga ja pakkuda koolitusi, mis efektiivselt tugevdavad teadlikkust ning parandavad kasutajate käitumist küberjulgeoleku valdkonnas (Nasir, 2023).

Soovitused tudengitele: Aktiivne osalemine küberjulgeoleku täiendkoolitustel ja seminaridel võib oluliselt suurendada tudengite ettevalmistuse taset ja teadlikkust küberohtudest. On oluline õppida ära tundma potentsiaalseid ohte ja arendada harjumust kriitiliselt hinnata internetis leiduvat informatsiooni ja ressursse (Antunes, 2021).

Soovitused õppeasutustele: Soovitused organisatsioonidele ja haridusasutustele hõlmavad ka õppekavade pidevat uuendamist ja kohandamist, mis arvestavad kaasaegse digitaalse maastiku nõudmisi (Corradini, 2020). Kasutades simuleerimisvahendeid nagu küberpolügoonid, saavad õpilased ja töötajad praktilist kogemust, mis on hindamatu küberrünnakutega toimetulekuks. Kaasaegsed õppijad peavad olema maksimaalselt teadlikud internetiruumis aktiivsusega seotud riskidest, kasutades digitaalseid seadmeid (Rahman, 2020). Lisaks peaksid õppeasutused pöörama erilist tähelepanu küberjulgeoleku praktilistele aspektidele, korraldades mängu või treeningseansse, mis aitavad paremini ette valmistuda reaalseteks küberohtudeks (Rahman, 2020; Karjalainen *et al.,* 2020). Mängustamine õppes aitab tõhusalt arendada praktilisi oskusi, mis on eriti oluline reaalsete väljakutsete ja olukordadega toimetulekuks professionaalses valdkonnas (Triplett, 2023).

Kiiresti muutuvate küberjulgeoleku nõuete tõttu tekib vajadus õppekavade kohandamiseks. Tudengite ja töötajate kaasamine küberjulgeoleku täiendkoolitustel ja seminaridel suurendab oluliselt nende teadlikkust ja ettevalmistust, aidates ära tunda potentsiaalseid ohte ja kriitiliselt hinnata internetis leiduvat informatsiooni. See kõik on osa laiemast strateegiast, mis käsitleb küberjulgeolekut kui pidevat ja integreeritud protsessi, kus

iga osaleja isiklik panus on hädavajalik. Lisaks rõhutab uuring pideva õppe tulemuste ja õppuste efektiivsuse hindamise olulisust ning vajadust välja töötada lihtsad, kuid komplekssed hindamisvahendid teadmiste kasvu tõhusaks mõõtmiseks ja koolitusprogrammide täiustamist vajavate valdkondade kindlakstegemiseks (Karjalainen *et al.,* 2020).

4.3 Tulemuste piirangud ja tulevased uurimissuunad

Vaadates saadud tulemuste tähtsust, on oluline arvestada minu uuringu piiranguid, sealhulgas keskendumist esmakursuslastele ja piiratud valimile. Tulevased uuringud peaksid püüdlema valimi laiendamise poole, et hõlmata laiemat ringi õppeasutusi ja erialasid. Samuti on oluline uurida uuendatud õppeprogrammide mõju tudengite teadlikkusele ja ettevalmistusele küberohtude osas.

Kokkuvõttes rõhutab käesolev uuring hariduse kriitilist rolli küberjulgeoleku kultuuri kujundamisel noorte seas. Koolide ees seisab ülesanne nii pakkuda tudengitele vajalikke teadmisi ja oskusi, kui ka inspireerida neid aktiivselt osalema turvalise digitaalse tuleviku loomises (Alrabaee, 2022). On oluline, et haridusasutused näeksid seda väljakutsena ja tudengid võimalusena isiklikuks ja professionaalseks arenguks valdkonnas, mis mängib võtmerolli meie digitaalse tuleviku turvalisuse tagamisel.

TÄNUAVALDUSED

Sügav tänu kõigile, kes on aidanud kaasa minu magistritöö valmimisele. Eriti tahan tänada oma magistritöö juhendajat Meeli Rannastu-Avalos, kelle juhendamisoskused, toetus ja asjatundlikkus olid asendamatud. Tema väärtuslikud nõuanded ja pühendunud suhtumine minu uurimuse arengusse on aidanud mul jõuda uuele teadmiste tasemele ning avardanud minu akadeemilist silmaringi.

Samuti tänan südamest kõiki õpetajaid, kelle erialased teadmised ja juhised on oluliselt rikastanud minu uurimistööd. Tänu kuulub ka keeletoimetajale, kelle professionaalne panus aitas tagada töö keelelise täpsuse ja selguse.

Eraldi tahan avaldada sügavat tänu oma perele, kelle toetus ja mõistmine on olnud minu jaoks hindamatu väärtusega kogu selle akadeemilise teekonna vältel.

AUTORSUSE KINNITUS

Kinnitan, et olen iseseisvalt koostanud käesoleva magistritöö, tuues esile kõik kasutatud allikad. Töö vastab Tartu Ülikooli Viljandi Kultuuriakadeemia lõputööde koostamise nõuetele ning on koostatud kooskõlas heade akadeemiliste tavadega.

Allkiri:
Kuupäev:

KASUTATUD KIRJANDUS

Abawajy, J. (2012). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33, 1-12. https://doi.org/10.1080/0144929X.2012.708787

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. *Big Data Cognitive Computing*, 5, 23. https://doi.org/10.3390/bdcc5020023

Alqahtani, M. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*. https://doi.org/10.3390/app12052589

Alrabaee, S., Al-kfairy, M., & Barka, E. (2022). Efforts and Suggestions for Improving Cybersecurity Education. In *2022 IEEE Global Engineering Education Conference (EDUCON)*, 1161-1168. https://doi.org/10.1109/EDUCON52537.2022.9766653

Antunes, M., Silva, C., & Marques, F. (2021). An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context. *Applied Sciences*, 11, 11269. https://doi.org/10.3390/app112311269

Bada, M., Sasse, A., & Nurse, J. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Presented at the *International Conference on Cyber Security for Sustainable Society*. https://www.researchgate.net/publication/274663655_Cyber_Security_Awareness_Campaigns_Why_do_they_fail_to_change_behaviour

Chang, L., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers and Security*. https://doi.org/10.1016/j.cose.2020.101959

Corradini, I. (2020). Developing Cybersecurity Awareness, 101-113. https://doi.org/10.1007/978-3-030-43999-6_6

Corradini, I. (2020). Building a Cybersecurity Culture, 63-86. https://doi.org/10.1007/978-3-030-43999-6_4

Digitaalse õppematerjali loomise põhimõtted. (s.a.). https://oppevara.edu.ee/kvaliteet/?_ga=2.63761263.1104080623.1620411550432037758.1619465146#oppematerjalide-valjatootamise-etapid

Erelt, T., Kadakas, M., Kala-Arvisto, U., Kraav, I., Maanso, V., Puksand, H., Tamm, E., & Unt, I. (2014). *Hariduse ja kasvatuse sõnaraamat. Haridussõnastik*. Eesti Keele Sihtasutus. http://www.eki.ee/dict/haridus/

Gallego-Arrufat, M., Torres-Hernández, N., & Pessoa, T. (2019). Competence of future teachers in the digital security area. *Comunicar*, 27, 57-67. https://doi.org/10.3916/c61-2019-05

Gartner. (2016). Measuring the strategic value of the internet of things for industries. https://www.gartner.com/doc/3299317

Hariduse tehnoloogiakompass (2023). *Harno*. https://kompass.harno.ee/

Haridus- ja Noorteamet. (2023). *Harno*. https://harno.ee/

Kanellos, L. (2020). *The GDPR Handbook*.

Karjalainen, M., Puuska, S., & Kokkonen, T. (2020). Measuring Learning in a Cyber Security Exercise. *Proceedings of the 12th International Conference on Education Technology and Computers*. https://doi.org/10.1145/3436756.3437046

KeeJoh O'Hearon, McKee M., Hossain N., & Canbaz M. (2021). IoT Privacy and Security in Teaching Institutions: Inside The Classroom and Beyond. *Indiana University Kokomo*. https://www.researchgate.net/publication/354867275_IoT_Privacy_and_Security_in_Teaching_Institutions_Inside_The_Classroom_and_Beyond

Kouroupis, K., & Vagianos, D. (2023). IoT in Education: Implementation Scenarios through the Lens of Data Privacy Law. *Journal of Politics and Ethics in New Technologies and AI*. https://www.researchgate.net/publication/371166334_IoT_in_Education_Implementation_Scenarios_through_the_Lens_of_Data_Privacy_Law

Kurzweil, D., & Baker, S. (2017). *The Internet of Things for Educators and Learners*. https://er.educause.edu/articles/2016/8/the-internet-of-things-for-educators-and-learners

Lella, I. (2023). *ENISA THREAT LANDSCAPE 2023*. European Union Agency for Cybersecurity (ENISA). https://doi.org/10.2824/782573

Lopez, J., Rios, R., Bao, F., & Wang, G. (2017). Evolving privacy: From sensors to the internet of things. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.04.045

Lueth, K. (2014). Why the Internet of Things is called Internet of Things: Definition, history, disambiguation. https://iot-analytics.com/internet-of-things-definition/

Madakam, S. jt (2015). Internet of Things: Literature Review. http://file.scirp.org/pdf/JCC_2015052516013923.pdf

Mai, P., & Tick, A. (2021). Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam. *Acta Polytechnica Hungarica*, 18, 67-89

Mason, O., Collman, S., Kazamia, S., & Boureanu, I. (2023). Preparing UK students for the workplace: The Acceptability of a Gamified Cybersecurity Training. *Journal of Cybersecurity Education Research and Practice*. https://doi.org/10.32727/8.2023.35

Meola, A. (2016). How IoT in education is changing the way we learn. http://www.businessinsider.com/internet-of-things-education-2016-9

Moallem, A. (2017). Do You Really Trust "Privacy Policy" or "Terms of Use" Agreements Without Reading Them? In Nicholson, D. (Ed.), *Advances in Human Factors in Cybersecurity, AHFE 2017, Advances in Intelligent Systems and Computing* (Vol. 593). Springer, Cham. https://doi.org/10.1007/978-3-319-60585-2_27

Moallem, A. (2018). Cyber Security Awareness Among College Students. In Ahram, T. (Ed.), *Advances in Human Factors in Cybersecurity, AHFE 2018, Advances in Intelligent Systems and Computing* (Vol. 782). Springer, Cham. https://doi.org/10.1007/978-3-319-94782-2_8

Nasir, S. (2023). Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions. *Advances in Multidisciplinary and Scientific Research Journal Publication*. https://doi.org/10.22624/aims/csean-smart2023p18

Nicholson, D. (Ed.). (2018). *Advances in Human Factors in Cybersecurity, AHFE 2018, Advances in Intelligent Systems and Computing* (Vol. 782). Springer, Cham. https://doi.org/10.1007/978-3-319-94782-2_8

Pătrașcu, P. (2019). Promoting Cybersecurity Culture through Education. https://www.researchgate.net/publication/368811952_PROMOTING_CYBERSECURITY_CULTURE_THROUGH_EDUCATION

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education. *IEEE Security & Privacy*, 18, 68-74. https://doi.org/10.1109/MSEC.2020.2969409

Pew Research Center. (2017). Americans and Cybersecurity. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Põhikooli riiklik õppekava (2023). https://www.riigiteataja.ee/akt/123042021010

PRAXIS. (2017). IKT-haridus: digioskuste õpetamine, hoiakud ja võimalused üldhariduskoolis ja lasteaias. https://www.praxis.ee/wp-content/uploads/2016/08/IKT-hariduse-uuring_aruanne_mai2017.pdf

Rahman, N., Sairi, I., Zizi, N., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information Education Technology*, 10, 378-382

Rao, U. (2023). Overview of Cyber Security. *International Journal of Advanced Research in Science, Communication and Technology*. https://doi.org/10.48175/ijarsct-9470

Raudla, H. (2019). Millest sõltub koolide digipädevus? *Õpetajate Leht*. https://opleht.ee/2019/03/millest-soltub-koolide-digipadevus

Riigi Infosüsteemi Amet. (2022). *Küberturvalisuse aastaraamat 2022*. https://www.ria.ee/media/1488/download

Riigi Infosüsteemi Amet. (2023). *Küberturvalisuse aastaraamat 2023*. https://www.ria.ee/media/2653/download

Rikk, R. (2018). Teadlane teab: Mis on küberturvalisus? https://www.tlu.ee/dt/uudised/teadlane-teab-mis-kuberturvalisus-raul-rikk

Risteska Stojkoska, B., & Trivodaliev, K. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, 140, Part 3, 1454-1464. https://doi.org/10.1016/j.jclepro.2016.10.006

Sam, M., Ismail, A., Abu Bakar, K., Amiruddin, A., & Qureshi, M. (2020). The Effectiveness of IoT Based Wearable Devices and Potential Cybersecurity Risks: A Systematic Literature Review from the Last Decade. *Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia (UTeM)*, Melaka, Malaysia. https://doi.org/10.3991/ijoe.v18i09.32255

Schaffer, D., & Debb, S. (2019). Validation of the Online Security Behaviors and Beliefs Questionnaire with College Students in the United States. *Cyberpsychology, Behavior, and Social Networking*. https://doi.org/10.1089/cyber.2019.0248

Sharma, A., & Sharma, R. (2020). A Review of Applications, Approaches, and Challenges in Internet of Things (IoT). In Singh, P., Kar, A., Singh, Y., Kolekar, M., & Tanwar, S. (Eds.), *Proceedings of ICRIC 2019. Lecture Notes in Electrical Engineering* (Vol. 597). Springer, Cham. https://doi.org/10.1007/978-3-030-29407-6

Silva, B. (2023). Exploring the Relationship Between Cybersecurity Culture and Cyber-Crime Prevention: A Systematic Review. *International Journal of Information Security and Cybercrime*. https://doi.org/10.19107/ijisc.2023.01.03

Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018). What is a smart device? - a conceptualisation within the paradigm of the internet of things. *Visualization in Engineering*, 6, 3. https://doi.org/10.1186/s40327-018-0063-8

Skarga-Bandurova, I., Kotsiuba, I., & Velasco, E. (2021). Cyber Hygiene Maturity Assessment Framework for Smart Grid Scenarios. *Frontiers in Computer Science*. https://doi.org/10.3389/fcomp.2021.614337

Smith, S. (2023). Towards a Scientific Definition of Cyber Resilience. *International Conference on Cyber Warfare and Security*. https://doi.org/10.34190/iccws.18.1.960

Tae, J. (2017). The Development and Application of a STEAM Program for Middle School Students Using an Internet of Things Teaching Aid. *Information: Tokyo*. https://search.proquest.com/openview/780278479a325ca5f05572f8f732fb12/1?pq-origsite=gscholar&cbl=93633

Tempestini, G., Rovira, E., Pyke, A., & Nocera, F. (2023). The Cybersecurity Awareness INventory (CAIN): Early Phases of Development of a Tool for Assessing Cybersecurity Knowledge Based on the ISO/IEC 27032. *Journal of Cybersecurity and Privacy*. https://doi.org/10.3390/jcp3010005

Triplett, W. (2023). Addressing Cybersecurity Challenges in Education. *International Journal of STEM Education for Sustainability*. https://doi.org/10.53889/ijses.v3i1.132

Vaks, T. (2013). Riigi Infosüsteemi Ameti kokkuvõte küberturvalisuse tagamisest 2012. https://www.ria.ee/media/1526/download

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2, The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes*. EUR 31006 EN, Publications Office of the European Union, Luxembourg. ISBN 978-92-76-48883-5. https://doi.org/10.2760/490274

Wang, Z., Zhu, H., & Sun, L. (2021). Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *Chinese Academy of Sciences*. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9323026

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). Internet of Things: A Survey of Topics & Trends. *Information Systems Frontiers*. https://pdfs.semanticscholar.org/705f/e9247176e3f891b249c49b08492c295e507d.pdf

Zaharakis, I., Sklavos, N., & Polychronopoulos, G. (2016). Exploiting Ubiquitous Computing, Mobile Computing and the Internet of Things to Promote Science Education. https://www.researchgate.net/profile/Nicolas_Sklavos/publication/310775960_Exploiting_Ubiquitous_Computing_Mobile_Computing_and_the_Internet_of_Things_to_Promote_Science_Education/links/5a194baa4585155c26a96f66/Exploiting-Ubiquitous-

Computing-Mobile-Computing-and-the-Internet-of-Things-to-Promote-Science-Education.pdf

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62, 1, 82-97. https://doi.org/10.1080/08874417.2020.1712269

Õunapuu, L. (2014). Kvalitatiivne ja kvantitatiivne uurimisviis sotsiaalteadustes. http://hdl.handle.net/10062/36419

LISAD

Lisa A. *Uurimusküsimuste küsimustik Eesti keeles*

1. Palun märkige oma vanus?

2. Milline on teie haridustase?
   - *Gümnaasium*
   - *Kutsekool*
   - *Muu:*

3. Millisel õppekaval te õpite?

4. Kui palju aega päevas veedate internetis, tegeledes tegevustega, mis nõuavad isikliku teabe vahetamist või paroolide kasutamist (näiteks sotsiaalmeedia, online-mängud, e-post)?
   - *üle 6 tunni päevas*
   - *4 kuni 6 tundi päevas*
   - *2 kuni 4 tundi päevas*
   - *1 kuni 2 tundi päevas*
   - *alla 1 tunni päevas*

5. Kuidas hindate oma enesekindlust järgmistes digipädevuse aspektides? Palun hinnake iga punkti "Üldse mitte enesekindel" kuni "Väga enesekindel":
   - *Teksti- ja tabeltöötlus (nt Word, Excel).*
   - *Andmekaitse internetis (privaatsus, GDPR).*
   - *Pilveteenused ja failide jagamine (Google Drive, Dropbox).*
   - *Sisuloomine ja -redigeerimine (video, graafika).*

- *Küberturvalisuse meetmed (sh kahefaktoriline autentimine).*
- *Info otsimine ja organiseerimine (otsingumootorid, andmebaasid).*
- *Digisane seits orientitet*
- *Autoriõigused ja litsentsia (teiste sisu kasutamine).*
- *Innovatsioon ja probleemide lahendamine (digivahendid, loovus).*

6. Kui tihti te arutate küberturvalisuse teemadel oma sõprade või perekonnaga?
   - *Väga sageli (peaaegu iga päev)*
   - *Sageli (mitu korda nädalas)*
   - *Aeg-ajalt (mitu korda kuus)*
   - *Harva (mitu korda aastas)*
   - *Peaaegu mitte kunagi*
   - *Ei aruta kunagi*
7. Kuidas hindate oma võimet kaitsta end soovimatute ja pahatahtlike veebikohtumiste ning materjalide eest?
   - *Ma ei tea, kuidas seda teha*
   - *Ma saan seda teha kellegi abiga*
   - *Ma saan seda teha iseseisvalt*
   - *Ma saan seda teha kindlalt ja vajadusel teisi juhendada*

8. Kui tõsiselt te suhtute küberturvalisuse ohudesse oma igapäevaelus?
   - *Väga tõsiselt*
   - *Tõsiselt*
   - *Mõõdukalt*
   - *Ei väga tõsiselt*
   - *Üldse mitte tõsiselt*

9. Millised tegevused aitavad teie arvates kõige tõhusamalt kaasa küberturvalisuse tõstmisele?
    - Riskide teadlikkuse ja koolituse osas: Usun, et iga kasutaja teadlikkus on küberturvalisuse võtmeks.
    - Tehnilised kaitsevahendid: Antiviiruste ja tulemüüride kasutamine peaks olema standardpraktika.
    - Tarkvara ja paroolide regulaarne uuendamine: Programmide ajakohasus ja keerukate paroolide kasutamine on turvalisuse alus, mille eest vastutavad nii tootjad kui ka kasutajad.
    - Tootjate ülesanne: Arvan, et küberturvalisuse eest peaksid vastutama seadmete tootjad ja rakenduste arendajad, kasutajad peaksid saama tooteid kasutada ilma lisamuretsemata.
    - Ei ole kindel / Raske öelda: On raske hinnata, millised meetmed on kõige tõhusamad.

10. Mis on klikimeedia peamine eesmärk?
    - *Meelitada ligi võimalikult palju liiklust*
    - *Desinformatsioon*
    - *Informatsiooni manipuleerimine*
    - *Takistada ebausaldusväärse informatsiooni levitamist sotsiaalvõrgustikes*
    - *Ma ei tea, mis on klikimeedia.*

11. Kas suudate tuvastada oma seadmes kahtlase rakenduse kaudsete märkide alusel?
    - *Ei, ma ei saa seda teha*
    - *Ma pole kindel*
    - *Jah, ma saan seda teha, kuid mitte alati kindlalt*
    - *Jah, ma suudan seda kindlalt teha*

- *Muu: _____*

12. Kas olete kunagi kogenud või tuvastanud pahavara oma seadmes? Kuidas te sellega toimisite?
    - *Jah, kasutasin viirusetõrjetarkvara probleemi lahendamiseks*
    - *Jah, pöördusin IT-spetsialisti poole*
    - *Ei, ei ole kunagi kogenud*
    - *Muu: _____*

13. Kas olete kokku puutunud õngitsuskirjade, -sõnumite või -kõnedega? Kuidas reageerisite?
    - Jah, tuvastasin need ja ei langenud ohvriks
    - Jah, kuid langesin lõksu
    - Ei ole kindel
    - Ei, ei ole kunagi kokku puutunud

14. Kas olete või on keegi teie tuttavatest kokku puutunud sotsiaalse manipulatsiooniga ja kuidas see mõjutas teie arusaama küberturvalisusest?
    - *Jah, see suurendas minu teadlikkust ja ettevaatlikkust*
    - *Jah, kuid see ei mõjutanud minu arusaama küberturvalisusest*
    - *Ei ole kindel, kas see oli sotsiaalne manipulatsioon*
    - *Ei, ei ole sellise olukorraga kokku puutunud*
    - *Ma ei tea, mis on sotsiaalne manipulatsioon.*

15. Kuidas saate kasutada oma seadme rakenduses lähedalasuvate kohtade otsingufunktsiooni?
    - *Juurepääs geolokatsioonile*
    - *Juurepääs kaamerale*

- *Juurepääs kontaktidele*
- *Juurepääs failidele ja meediale*

16. Kui tihti uuendate oma seadmete tarkvara ja rakendusi?
    - *Iga kord, kui uuendus on saadaval*
    - *Korra kuus*
    - *Ainult siis, kui on probleeme seadme kasutamisega*
    - *Harva või mitte kunagi*

17. Kui hästi olete informeeritud küberturvalisuse meetmetest?
    - *Väga hästi informeeritud: Tunnen küberturvalisuse meetmeid põhjalikult ja olen kursis uusimate arengutega.*
    - *Piisavalt informeeritud: Mul on hea ülevaade küberturvalisuse meetmetest, kuigi võin mitte olla teadlik kõige uuematest arengutest.*
    - *Nõrgalt informeeritud: Tean mõningaid küberturvalisuse põhitõdesid, kuid minu teadmised on piiratud.*
    - *Ei ole informeeritud: Mul puuduvad teadmised küberturvalisuse meetmetest.*
18. Milliseid ressursse peate kõige usaldusväärsemaks küberturvalisuse alase teabe saamiseks?
    - *Ametlikud valitsuse veebilehed*
    - *Haridusasutuste materjalid*
    - *Eksperdiblogid ja foorumid*
    - *Sotsiaalmeedia*
    - *Muu: _____*

19. Milliseid ettevaatusabinõusid rakendate, kui ühendate oma seadme avaliku WiFi-võrguga?

- *Kasutan VPN-i*
- *Ei ühenda oma seadet avalike WiFi-võrkudega*
- *Piiran teatud tegevusi (nt pangandus või ostud)*
- *Muu: _____*

20. Kuidas hindate oma võimet tuvastada, kas veebileht/rakendus, kus teilt palutakse isikuandmeid, on turvaline (nt https, turvalisuse logo või sertifikaat)?
    - *Ma ei tea, kuidas seda teha.*
    - *Ma saan seda teha kellegi abiga.*
    - *Ma saan seda teha iseseisvalt.*
    - *Ma saan seda teha kindlalt ja vajadusel teisi juhendada.*

21. Kas kontrollite oma sotsiaalmeedia ja teiste veebikontode privaatsusseadeid?
    - Regulaarselt
    - Mõnikord
    - Harva
    - Mitte kunagi

22. Millised mobiilseadmetega seotud küberriskid on teile teada? Kas oskate kirjeldada tüüpilist petukirja või sõnumit, millega olete kokku puutunud?
    - *Olen teadlik mitmesugustest mobiilseadmetega seotud küberriskidest, nagu pahavara, andmepüük (phishing), võltsrakendused ja võrguühenduse ohud. Lisaks olen kokku puutunud tüüpiliste petukirjade või sõnumitega, mis võivad sisaldada kahtlaseid linke, palveid isikliku teabe jagamiseks või petlikke võitlusteadete.*
    - *Ma tean põhilisi mobiilseadmetega seotud küberriske, nagu viirused ja petturlikud e-kirjad või SMS-sõnumid, kuid minu teadmised ei ole väga põhjalikud. Olen kogenud mõningaid petukirju või sõnumeid, mis võivad sisaldada eksitavaid nõudmisi või kahtlaseid pakkumisi.*

- *Olen teadlik mõnest üldisest mobiilseadmetega seotud riskist, nagu viirused või petturlikud rakendused, kuid minu kogemused ja teadmised selles valdkonnas on piiratud. Olen vaid mõned korrad kokku puutunud kahtlaste e-kirjade või sõnumitega.*
- *Ma ei ole eriti teadlik mobiilseadmetega seotud küberriskidest ja ei ole seni kogenud petukirju või sõnumeid. Minu kogemused selles valdkonnas on väga piiratud.*
- *Ma ei ole teadlik mobiilseadmetega seotud küberriskidest ega ole kunagi kokku puutunud petukirjade või sõnumitega. Mul puudub kogemus selles vallas.*

23. Mida teeksite, kui saaksite teada, et teie isikuandmetele on ebaseaduslikult ligi pääsetud?
    - *Teataksin sellest võimudele*
    - *Muudaksin oma paroole*
    - *Kontrolliksin oma kontode turvasätteid*
    - *Muu:* _____

24. Kuidas te reageeriksite, kui saaksite e-kirja, mis näib olevat teie panga poolt saadetud, kuid milles palutakse teil jagada oma isikuandmeid või pangakonto detaile?
    - *Kontrolliksin e-kirja autentsust, võttes ühendust pangaga otse*
    - *Järgiksin e-kirjas olevaid juhiseid, kui see tundub usaldusväärne*
    - *Eiraksin e-kirja ja märgiksin selle rämpspostiks*
    - *Muu:* _____

25. Ma uuendan regulaarselt oma teadmisi küberturvalisuse valdkonnas.
    - *Täiesti nõus*
    - *Pigem nõus*
    - *Neutraalne*
    - *Pigem ei ole nõus*
    - *Üldse ei ole nõus*

26. Kuidas tagate oma paroolide ja isikuandmete turvalisuse internetis? (Valige kõik sobivad vastused)

- *Kasutan paroolihaldurit paroolide hoidmiseks ja genereerimiseks*
- *Muudan regulaarselt kõikide oma kontode paroole*
- *Kasutan erinevaid paroole erinevate kontode jaoks*
- *Eelistan kasutada ainult kontrollitud ja turvalisi veebilehti*
- *Säilitan paroole oma veebibrauseris*
- *Kasutan kahefaktoriline autentimine*
- *Ei kasuta täiendavaid tööriistu ega meetmeid paroolide ja andmete turvalisuse haldamiseks*
- *Muu*

27. Kuidas te hindate internetis leiduva info usaldusväärsust ja kontrollite veebilehtede turvalisust enne isikuandmete sisestamist? Palun vastake, arvestades, kui tihti te kontrollite allikaid ja veebilehtede turvalisust enne isikuandmete sisestamist:

- *Ei kontrolli kunagi ei info usaldusväärsust ega veebilehtede turvalisust.*
- *Kontrollin mõnikord info usaldusväärsust, aga harva pööran tähelepanu veebilehtede turvalisusele.*
- *Regulaarselt kontrollin info usaldusväärsust ja mõnikord veebilehtede turvalisust.*
- *Alati põhjalikult kontrollin nii info usaldusväärsust kui ka veebilehtede turvalisust enne isikuandmete sisestamist.*

28. Milliseid turvameetmeid olete seadistanud oma nutiseadmetes ja arvutites, et kaitsta end küberohtude eest? (Mitmekordne valik)

- *Paigaldan ainult usaldusväärsete arendajate tarkvara*
- *Kontrollin kontosid andmete lekkimise suhtes*

- *Uuendan regulaarselt oma seadet ning operatsioonisüsteemi ja rakendusi*
- *Kasutan viirusetõrjeprogrammi*
- *Ei kasuta avalikke WiFi-võrke ilma VPN-ita, kasutan VPN-i*
- *Vältin sõnumites olevatele kahtlastele linkidele klõpsamist*
- *Ei ava kahtlaseid e-kirja manuseid*
- *Loen täielikult läbi konfidentsiaalsuspoliitika ja andmetöötluse lepingud*
- *Ei kasuta täiendavaid turvameetmeid / Mul ei ole midagi muretseda*

29. Minu kooliprogramm on mind küberturvalisuse riskide ületamiseks ette valmistanud.
    - *Täiesti nõus*
    - *Pigem nõus*
    - *Neutraalne*
    - *Pigem ei ole nõus*
    - *Üldse ei ole nõus*

30. Millised teemad või valdkonnad küberturvalisuses vajaksid teie arvates rohkem tähelepanu teie ülikooli õppekavas?
    - *Andmepüük ja sotsiaalne manipuleerimine*
    - *Turvalised online-maksetehnikad*
    - *Isikuandmete kaitse sotsiaalmeedias*
    - *Turvaliste paroolide loomine ja haldamine*
    - *Muu: _____*

SUMMARY

Cybersecurity awareness and attitudes among first-year students: a case study of three Estonian higher education institutions.

In today's rapidly advancing technological landscape, the ubiquitous integration of technology into daily life significantly heightens the relevance of cybersecurity. This master's thesis delves into evaluating the level of cybersecurity awareness and attitudes among first-year students at three prominent Estonian universities.

The objective of this research was to analyze students' self-assessment concerning their knowledge and perception of cybersecurity principles and risks, as well as their attitudes towards the importance of cybersecurity and their role in ensuring digital security. A particular focus was placed on the utilization of smart devices, which are integral to students' everyday activities.

The methodology employed in this study included a quantitative analysis through a structured questionnaire designed to assess students' knowledge and attitudes toward cybersecurity. The analysis indicated that, despite the extensive use of digital technologies, many students do not feel sufficiently prepared to face actual cyber threats, highlighting an urgent need for comprehensive cybersecurity education across all academic programs.

The principal findings from this study confirmed that the proactive incorporation of cybersecurity subjects into educational curricula significantly enhances students' readiness. Additionally, the data demonstrated that students enrolled in technical disciplines tend to have a higher awareness of cybersecurity risks and principles compared to their peers in the humanities. It is crucial to acknowledge that while this study identifies statistical correlations between various factors, it does not establish causal relationships.

The limited sample size and lack of experimental interventions not only restrict the ability to draw definitive conclusions about causality but also diminish the generalizability of the study's outcomes, underscoring the need for further and broader studies to assess the effectiveness of revised educational programs on students' preparedness levels.

This research underscores the necessity to tailor educational programs to the digital era's demands by incorporating a holistic approach to cybersecurity instruction, recommending the development and implementation of comprehensive educational strategies.

These strategies aim to enhance digital literacy and cybersecurity awareness among all student groups, enabling them to better comprehend the risks associated with digital technologies and respond more effectively to cyber threats in their future professional endeavors.

LIHTLITSENTS

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks
Mina, German Jaska,

1. Annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose Esmakursuslaste küberturvalisuse teadlikkus ja suhtumised kolme Eesti kõrgkooli näitel, mille juhendaja on Meeli Rannastu-Avalos, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.
2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.
3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.
4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

German Jaska
19.05.2024