TARTU ÜLIKOOL
Arvutiteaduse instituut
Informaatika õppekava

Omar Purik

Praktiliste ülesannete koostamine gümnaasiumile teemal „Infoturve“

Bakalaureusetöö (9 EAP)

Juhendajad: Kristjan Krips, MSc
Tauno Palts, MA

Tartu 2019

Praktiliste ülesannete koostamine gümnaasiumile teemal „Infoturve“

Lühikokkuvõte:

Bakalaureusetöö raames koostati õppematerjalid gümnaasiumiastme valikkursusena praktilise infoturbe õpetamiseks. Valmis neljateistkümnest topeltunnist koosnev kursus, mis keskendub Windows 10 turvamisele, kuid käsitleb ka veebibrausereid, Linuxit ning nutiseadmeid. Ülesannetes tutvustatavad rakendusprogrammid ning sätted aitavad kaitsta aktuaalsete infoturbe ohtude vastu ning materjalides jagatavaid juhiseid saab rakendada ka väljaspool kursust oma seadmeid turvates.

Võtmesõnad:

Infoturve, privaatsus, õppematerjalid, Windows 10, veebibrauserid

CERCS: P175 Informaatika, süsteemiteooria

Creation of Practical Assignments on Information Security for High School students

Abstract:

The purpose of this thesis was to create study materials for teaching practical information security to high school students. A course consisting of fourteen 90-minute lessons was designed and completed. The assignments focus mainly on securing Windows 10, but there are topics about configuring web browsers, Linux and mobile computing devices. Application software and configuration changes presented during these assignments helps to defend against information security threats and can be applicable outside this course for securing devices and information.

Keywords:

Information security, privacy, teaching materials, Windows 10, web browsers

CERCS: P175 Informatics, system theory

Sisukord

1. Sissejuhatus

Lõputöö eesmärgiks on luua praktiline ülesandekogu infoturbe teemalise gümnaasiumiastme valikkursuse jaoks. Esialgse kava kohaselt kasutatakse valminud õppematerjale Tartu Ülikooli õpetajakoolituse raames tulevaste informaatikaõpetajate infoturbe pädevuste suurendamiseks. Õpetajad saavad hiljem gümnaasiumiõpilastele kursust läbi viies loodud materjale kasutada või aluseks võtta. Ülesanded on koostatud eeldusega, et õpetajad on läbinud Tartu Ülikooli aine "Infoturve", kuid õpilastel varasemad infoturbe alased teadmised puuduvad.

Materjal on koostatud ühe 35 akadeemilisest tunnist koosneva gümnaasiumikursuse jaoks. Töömaht jaotub neljateistkümneks topelttunniks, mis koosnevad kahest 45-minutilisest koolitunnist. Seetõttu katab loodud materjal 80% (28 tundi) kursuse mahust. Iga tund koosneb lühikesest teoreetilisest sissejuhatusest ning praktiliste ülesannete lahendamisest, eesmärgiga anda õpilastele ülevaade peamistest infoturbe probleemidest ning nende tuvastamisest.

Õppematerjalid sisaldavad rohkelt ekraanitõmmiseid, et anda ülesannetest parem ettekujutus ning selgitada vajalikke tegevusi. Keskendutakse peamiselt Windows 10 operatsioonisüsteemile ja veebibrauseritele, kuid kasutatakse ka Linuxit (Ubuntu 18.04) ning levinumaid mobiil-operatsioonisüsteeme (Android ja iOS). Lisaks on paljud kursuses kasutatavad rakendusprogrammid platvormiülesed ehk saadaval ka näiteks macOS-ile. Ka Windowsi seadistamise ülesannetes käsitletakse valdkonna põhiprintsiipe, mis on enamasti sarnaselt rakendatavad ka teiste operatsioonisüsteemide puhul.

Kursuse raames õpetatavad meetodid ning kasutatavad tööriistad on kasulikud kõigile privaatsust hindavatele inimestele. Koostatud materjalide abil saab õppida praktilisel viisil virtuaalmaailmas andmete ning suhtluse turvamist. Muuhulgas käsitletakse kasutajate võrguidentiteedi kaitsmist, anonüümsuse säilitamist internetis, andmete krüpteerimist nii oma seadmes kui transpordiks, isiklike seadmete turvamist, pahavara ohvriks sattumise vältimist ning digitaalse jalajälje vähendamist.

2. Infoturbest

See peatükk kirjeldab esmalt, mis on infoturve, miks see oluline on ning miks seda gümnaasiumiastmes vaja õpetada on. Peatüki lõpus antakse ülevaade olemasolevatest õppematerjalidest ning selgitatakse lõputöö käigus valmiva materjali vajadust ning eripära ja erinevust eksisteerivatest eestikeelsetest materjalidest.

2.1 Infoturbest üldiselt

Infoturve on teabe ning infosüsteemide kaitsmise protsess, mille eesmärk on tagada kaitse teabe volitamata ligipääsu, kasutuse, avalikustamise, katkestuse, muutmise, salvestamise ning kustutamise eest [1]. Samaaegselt peaks turve olema võimalikult efektiivne ja kasutaja tööd mitte häirima, kuigi turvalisus ja produktiivsus on tihti diametraalsed vastandid. Sajaprotsendilist turvalisust pole kunagi võimalik tagada, kuid hästi turvatud süsteem teeb ründajatele ligipääsu nii keeruliseks, et nurjuvad enamik katsetest infole ligi pääseda [2].

Infoturbe põhiprintsiibid

Infoturbe probleemidest või situatsioonidest rääkides on kasulik omada mudelit, mille järgi seda teha. Enamasti on valdkonna mudelites keskesel kohal turvakolmik (ingl *CIA triad*), mida paljudel juhtudel käsitletakse osana infoturbe definitsioonist [1]. Selle järgi on infoturbe põhieesmärgiks info ja andmete konfidentsiaalsuse, käideldavuse ning tervikluse säilitamine. Kaitsemeetmete kasutamise eesmärk on enamasti mõnda neist kindlustada ning riske turvalisusele saab hinnata võime järgi neid printsiipe ohtu seada [3].

1. **Tervikluse** (ingl *integrity*) eesmärk on tagada informatsiooni ning süsteemide täpsus ja usaldusväärsus ning takistada lubamatuid muudatusi.
2. **Käideldavuse** (ingl *availability*) eesmärk on tagada süsteemide töökindlus ning õigeaegne ligipääs andmetele ning ressurssidele selleks volitatud isikutele.
3. **Konfidentsiaalsuse** (ingl *confidentiality*) eesmärk on tagada informatsiooni piisav salastatuse tase ning takistada ligipääs volitamata isikutele.

Ründed

Rünnatakse praktiliselt kõiki tarkvarakihte ja tasemeid võrguprotokollidest rakendusprogrammideni. Potentsiaalne kasu ründajatele võib olla tohutu ning tulevikus on oodata rünnete kasvu [4]. Valdava osa ründajate jaoks on peamine motivatsioon raha, kuid peale finantshuvide on ka muid põhjuseid nagu luure- ja mõjutustegevus ning privaatsetele või

konfidentsiaalsetele andmetele ligipääsemine [2]. Lisaks soovivad mõned ründajad informatsiooni varastada konkurentsieelise saamiseks või maine hävitamiseks.

Kinnisründeohud

Kinnisründeoht (ingl *advanced persistent threat* ehk APT) on välisriigi poliitilistest, majanduslikest või sõjalistest huvidest lähtuv ning ettemääratud eesmärgi saavutamisele suunatud ulatuslike ressursside ning erioskustega kestusründe oht [5].

Silmapaistev näide on Põhja-Korea, mille sõjaväe ning luureorganisatsiooniga seotud gruppe süüdistatakse muuhulgas WannaCry lunavara loomises, Bangladeshi pangast 81 miljoni dollari varastamises ning kättemaksuks Kim Jong-uni pilava komöödia eest Sony Picturesi andmete lekitamises [6]. Ainuüksi vähem kui kahekümnest kõrgkvalifikatsiooniga kräkkerist ehk pahatahtlikust häkkerist koosnev salalik grupp APT 38 tõi 2018. aastal Põhja-Korea majandusele sisse ligi miljard eurot. Varastatud raha kasutatakse peamiselt riigi sõjaliste operatsioonide (sealhulgas tuumarelvade) rahastamiseks [7].

Ründeid korraldavad ka demokraatlikud riigid. Ebatavaliselt keerukas oli 2010. aastal avastatud Stuxneti uss (isepaljunev kahjurvara), mis nakatas Windowsi kasutavaid seadmeid. See kasutas ära nelja nullpäeva turvaauku ehk nõrkust, millest tarkvara valmistaja ja viirusetõrjed veel teadlikud pole. Seetõttu oli seadmeid Stuxneti eest ka väga raske kaitsta. Ussi sihtmärgiks oli Iraani tuumakütuse rikastamise tehas, milles kasutatavad tehniliste protsesside jälgimise ja juhtimise seadmed (SCADA süsteem) polnud internetti ühendatud. Uss levis sülearvutite ning mälupulkade kaudu ning sellel õnnestus riigi tuumaprogrammile suurt kahju tekitada. Stuxnet kiirendas tsentrifuuge üle nende piirkiiruse, mis põhjustas ligi tuhande uraani rikastamise tsentrifuugi hävinemise. Seejuures ei olnud Iraani insenerid teadlikud, et nad rünnaku all on, kuna uss saatis seireseadmetele võltsandmeid. Kolm aastat hiljem lekkinud dokumendid kinnitasid, et Stuxnet oli Ameerika Ühendriikide ja Iisraeli loodud küberrelv [8].

Kaitse

Arvutite loomisest alates on turvalisus tihti järelmõtteks jäänud. Kuni üheksakümnendate alguseni oli interneti ärikasutus vähelevinud ning kasutajad olid peamiselt teadus-, haridus- ja valitsusasutused. Väiksest kasutajaskonnast tingituna oli omavaheline usaldus suurem ning kommertsteenuste puudumise tõttu ründajate motivatsioon väiksem. Tänaseks on

internetikasutajate arv tõusnud 4,53 miljardini[1] ning globaalselt investeeritakse infoturbesse üle 100 miljardi euro aastas [9]. Ründeid see peatanud pole, kuna kasutusel olevad süsteemid on tohutult keerulised ning kõikide nõrkuste parandamine on praktiliselt võimatu. Arvutisüsteemide olemuse tõttu piisab ründajatel sageli ainult ühe turvaaugu leidmisest. Samas eeldatakse kaitsjatelt, et nad suudaksid kõik turvavead tuvastada ja parandada. Ründajad saavad täielikult keskenduda ühele ründetüübile, aga kaitsja peab kõigiks valmis olema [2].

Turvalisust ei peeta tihti kõige tähtsamaks – esmalt soovitakse töötavat seadet paljude funktsioonidega ja alles seejärel mõeldakse turvalisusele, kuna turvameetmete valik ja teostamine nõuab palju raha ning vilumust, kuid ei paranda kasutajakogemust. Tihti on turbemeetodid pigem kasutust piiravad, aga kasutajad eelistavad efektiivsemaid ja lihtsamaid seadmeid või tarkvara [3].

Absoluutset turvalisust ei ole võimalik saavutada ning seega tuleb teha kompromisse. Ka turvateadlikud kasutajad hindavad ohte erinevalt, mistõttu peab iga inimene või organisatsioon leidma enda jaoks sobivaimad turvameetmed. Kasutaja enda tegevus on sageli suurimaks ohuks tema turvalisusele. Edukas infoturbe tagamine ei ole ainult ühekordne tegevus. See on protsess, mis võtab aega ning nõuab muutustega kursisolekut [10].

Turvalisusest tuleks mõelda kihtidena. Ühest kihist läbimurdmisel peaks teine ründe peatama või selle tuvastamist kergendama. Seejuures on oluline ka minimaalõiguste printsiip, mis on pääsupoliitika põhimõte, mille kohaselt peaks iga subjekt ehk isik, üksus või protsess omama minimaalseid lubatavaks tegevuseks vajalikke õigusi [5]. See tähendab, et administraatoriõigustes tuleks käivitada ainult need programmid, mis seda tõesti vajavad ning mida täielikult usaldatakse. Kuid ka tavakasutaja õigustega käivitatav programm pääseb tavaliselt ligi selle kasutajakonto failidele (näiteks dokumentidele) ning seetõttu tuleb iga täitmisfailiga ettevaatlik olla ning tundmatutest või ebausaldusväärsetest allikatest pärit tarkvara võimalusel vältida või käivitada ainult täiendavaid turvameetmeid kasutades. Eriti suur oht varjatud kahjurvara paigaldamiseks on piraattarkvara puhul, kuna illegaalsete võtmegeneraatorite ning paikade kasutamine nõuab tihti viirusetõrje väljalülitamist või erandite lisamist. Piraattarkvarale tehtud muudatustest puudub ülevaade ning kuigi loojate ning üleslaadijate poolt levitatakse väiteid, et neist kahjurvara leidmisel on tegu väärtuvastusega, ei saa selles kunagi kindel olla. Samuti ei võimalda need sageli tarkvara edaspidist uuendamist, mis turvanõrkuste avastamise korral samuti seadmele ohtu kujutab [11].

[1] https://www.internetworldstats.com/stats.htm

Ohumudel

Tähtis komponent info turvamisel on ohumudel (ingl *threat model*). See aitab määrata sobiva turvataseme teabe efektiivseks kaitsmiseks. Oluline on keskenduda tegelikele ning tõenäolistele ohtudele, kuna selget sihti omamata on raske seadmeid kaitsta [12].

Skriptinagad (ingl *script kiddie*) ehk häkkerikultuuris võhiklikud (aga pahatahtlikud) arvutikasutajad sooritavad oskuste puudumise tõttu ründeid teiste loodud kahjurvaraga ning oportunistlikult. Sellised ründajad on pahatahtlikest ekspertidest oluliselt levinumad. Kui ei ole vajadust või soovi konkreetse isiku või seadme ründamiseks valitakse ohvriks kõige kergemini ligipääsetavad sihtmärgid. Seetõttu aitab juba elementaarsete turvameetmete kasutamine ennetada suurt osa rünnakutest.

Sihtrünne (ingl *targeted attack*) on seevastu spetsialiseeritud konkreetsele isikule, organisatsioonile, süsteemile või tarkvarale. Kui ründajaks on ulatuslikke ressursse ja globaalset haaret omavad riiklikud küberründeüksused või muu ekspertidest koosnev grupp, on seadmeid keskendatud sihtründe eest praktiliselt võimatu kaitsta. Võimalus, et keskmine arvutikasutaja selliste ründajate huviorbiiti satub on kaduvväike, kuid ründajate võimekuse teadmine aitab valdkonda paremini mõista. Ründajate jaoks on kõik internetti ühendatud seadmed sekundi murdosa kaugusel ning operatsioonisüsteemis või tarkvaras avastatud turvanõrkus võib ohtu seada kõik selle kasutajad [13].

Privaatsusprobleemid ja massjälitus

Privaatsus tähendab inimese õigust kontrollida tema kohta käiva isikliku teabe avaldamist ja kasutamist. Kuigi privaatsusprobleeme leidus juba enne arvutite (või isegi kirjakeele) loomist, tegid suure arvutusvõimsusega seadmed võimalikuks suuremahulise andmete kogumise ja nendest seoste leidmise. Kuna privaatsus on osa konfidentsiaalsusest, on see üks aspekt infoturbest.

Isikuandmete kaitse üldmäärus

Isikuandmete kaitse üldmäärus (ingl *General Data Protection Regulation* ehk GDPR) on Euroopa Liidu määrus, mis jõustus 2018. aasta mais [14]. Lisaks üleeuroopalisele andmekaitse ühtlustamisele sätestas see printsiibi, mille kohaselt peavad üksikisikud saama otsustada kuidas nende kohta käivaid andmeid kasutatakse. Samuti sunnib määrus firmasid andmete töötlemist ning levitamist põhjendama. GDPR kehtib kõikidele ettevõtetele ja asutustele, mis koguvad või töötlevad Euroopa Liidu elanike isikuandmeid, mistõttu on selle mõju

ülemaailmne. Määrus kaitseb andmeid, mille abil kasutajaid identifitseerida saab, seetõttu katab see ka näiteks IP-aadresside ning asukohaandmete kasutamist. Määruse rikkumise korral ähvardab ettevõtteid ja asutusi trahv, mille suuruseks on kuni 4% aastasest käibest.

Edward Snowden

Suur osa massjälituse kohta käivast infost on tänaseni salastatud, kuid 2013. aastal lekitas endine Ameerika Ühendriikide Riikliku Julgeolekuagentuuri (NSA) ning Luure Keskagentuuri (CIA) lepinguline töötaja Edward Snowden ajakirjanikele suures koguses ülisalajase kitsenduspiiranguga teavet.

Esimesena avaldati 6. juunil The Guardianis kohtumäärus, mille kohaselt olid Föderaalne Juurdlusbüroo (FBI) ja NSA kogunud infot 120 miljoni telekommunikatsioonikonglomeraadi Verizoni kliendi kõneajaloo kohta (osapoolte asukoht, kõne aeg, kestus). Järgmisel päeval paljastati PRISM koodnimega järelevalvetegevus, mille raames koguti suurfirmade Microsoft, Google, Yahoo!, Facebook, PalTalk, Youtube, Skype, AOL ning Apple kasutajate andmeid, e-kirju, reaalajas teksti- ja videovestlusi, sisselogimisi, salvestatud andmeid ja faile ning eritaotlustega ka muud infot. Lisaks avalikustati veel mitu järelevalveprogrammi, mille eesmärk oli koguda globaalselt kasutajate internetikasutuse ajalugu ning sisu selle hilisemaks töötlemiseks ning arhiveerimiseks [15].

Kogutud andmed võimaldasid NSA töötajatel näiteks nime, e-posti- või IP-aadressi sisestamisega jälgida reaalajas praktiliselt iga internetikasutaja tegevust, asukohta, kasutusajalugu ning kontakte.

Glenn Greenwald ja tema töökaaslased said sellest tehtud reportaažide eest Pulitzeri preemia avaliku teenistuse kategoorias ning Laura Poitrase film “Citizenfour”, milles Snowdenit dokumentide avalikustamise ajal intervjueeriti, parima dokumentaalfilmi Oscari.

Inimesed peaksid teadma kuidas enda kohta käivaid andmeid kaitsta ning privaatsust tagada. Laialt on levinud arvamus, et massjälitus ei põhjusta kahju – ainult inimestel, kes tegelevad halbade asjadega, on midagi varjata. Sellest järeldub kaudselt, et maailmas on ainult kahte liiki inimesi - head ja halvad. Lisaks saab juba massjälituse definitsiooni põhjal öelda, et suuremat kahju põhjustab see ühiskonnast valdava osa moodustavale süütutele inimestele

Põhjus, miks inimesed privaatsust praktiliselt universaalselt ja instinktiivselt soovivad seisneb psühholoogias. Olukorras, kus meid jälgitakse muutub käitumine dramaatiliselt – potentsiaalsete valikute hulk väheneb ja on oluliselt konformistlikum. See on fakt

inimloomusest, mida on tõestanud kümned psühholoogiauuringud ning tunnistatud praktiliselt igas valdkonnas. Potentsiaalse häbi tõttu tehakse otsuseid, mis ei põhine enda soovidel, vaid ühiskondlikel ootustel [16].

Privaatsusmeetmete rakendamisega väheneb ka võimalus inimeste kontrollimiseks või mõjutamiseks [17].

Google

Umbes 95% Euroopa internetiotsingutest tehakse Google'i otsingumootorit kasutades [18]. Lisaks kuulub Google'ile maailma populaarseim operatsioonisüsteem (Android), veebibrauser (Google Chrome), videojagamisplatvorm (YouTube), kaarditarkvara (Google Maps), e-posti teenus (Gmail) ning palju muid sadade miljonite kasutajatega teenuseid.

Enamik lõppkasutajale suunatud teenustest on tasuta, kuid ometi oli Google'i emafirma Alphabet Inc.-i netokasum 2018. aastal üle 30 miljardi USA dollari. Firma käibest üle 85 protsendi moodustab nende interneti suurim reklaamivõrgustik Google Ads[2].

Veebilehtede külastamisel ei laeta sisu ainult aadressiribal olevalt domeenilt. Näiteks 2015. aastal läbiviidud uuringu kohaselt saadab brauser enam kui 78% veebilehtede külastamisel päringuid ka Google'ile [19]. Valdava osa sellest moodustab veebianalüüsi teenus Google Analytics, mis pakub veebisaitide omanikele põhjalikku statistikat külastajate kohta. Google pole muidugi ainus firma, mis massiliselt ja kasutajate jaoks varjatult andmeid kogub, kuid on kahtlemata turu kõige suurem [20].

Erinevatest allikatest pärit andmete kombineerimine annab Google'ile ülevaate miljardite kasutajate tegevusest internetis. Isegi Androidi, Google'i konto ning Google Chrome'i vältimisel saadavad ka paljud iOS-i rakendused Google'ile suures koguses andmeid. Andmete kogumist on kasutajate eest varasemalt ka varjata püütud ning seetõttu pole paljud kasutajad kogutava andmehulga ulatusest teadlikud [21].

Kasutajate andmed on aluseks internetireklaamidele, mille turg oli 2018. aastal üksnes Ameerika Ühendriikides ligi sada miljardit eurot. Valdav osa sellest tuleb kasutajate tähelepanu müümisest personaliseeritud reklaamide näol [18]. See toimib peamiselt läbi reaalajas enampakkumiste süsteemide, mis on avatud kõigile maksta soovivatele isikutele. Need saadavad kasutajate andmeid tundmatutesse sihtkohtadesse sadu miljardeid kordi päevas.

[2] https://ads.google.com

Seejuures on kaasatud andmete hulk oluliselt suurem kui see, mis saadakse häkkimiste ning andmelekete tagajärjel [22].

Windows 10

Kaitsemeetmete eduka rakendamise eelduseks on see, et operatsioonisüsteemi ei ole eelnevalt õõnestatud. Pahavaraga nakatunud või tagauksi omav operatsioonisüsteem muudab kaitsetuks kõik selles käivitatavad rakendused ning andmed. Siiski on olukord paranenud programmide õiguste ning failisüsteemile ligipääsu piiramisega [23].

Operatsioonisüsteemi turvalisemaks konfigureerimine on tähtis samm digitaalse privaatsuse ning turvalisuse kaitsmiseks. Kuigi Windows 10 sisaldab palju uusi või täiendatud turbevahendeid, põhjustas selle väljatuleku järgselt tulist arutelu hoopis vaikimisi valitud privaatsussätted [11].

Windows 10 kogub võrreldes varasemate versioonidega kasutajate kohta oluliselt rohkem andmeid ning saadab neid Microsoftile. Milliseid andmeid kogutakse sõltub tehtavatest valikutest, privaatsussätetest ning kasutatavatest funktsioonidest. Microsofti privaatsusavalduse[3] kohaselt tuletatakse teavet interaktsioonide, kasutuse ja kogemuse põhjal firma toodetega ning kogutakse andmeid kolmandatelt osapooltelt. Kõige rohkem kogutakse andmeid Cortana (Windowsi integreeritud digitaalne assistent) kasutamisel, mis salvestab klahvivajutusi, otsinguid, oste, kuulatavat muusikat, kalendri andmeid ja palju muud. Firma sõnul tehakse seda eelkõige kasutuskogemuse personaliseerimiseks, kuid ekspertidel olid erinevad ning vastukäivad arvamused [24]. Nimekiri telemeetria (kaugseire) kaudu saadetavatest andmetest avalikustati alles 2017. aasta aprillis, kakskümmend kuud pärast operatsioonisüsteemi müügiletulekut [24].

Siiski peetakse Windows 10-t jätkuvalt turvaliseks ja töökindlaks operatsioonisüsteemiks ning täiendava sätete muutmise ja süsteemi tugevdamisega saab selle privaatsussõbralikumaks muuta. Kriitika tõttu on Microsoft uuendustega privaatsussätted arusaadavamaks ning lihtsamini muudetavaks teinud.

Anonüümsus

Näilikkusest hoolimata pole internet kunagi anonüümne vahend olnud. Seda arvestamata käituvad inimesed tihti nagu nad oleksid anonüümsed, postidades veebisaitidele

[3] https://privacy.microsoft.com/et-ee/privacystatement

ebameeldivaid kommentaare ning külastades “inkognito” või “privaatse sirvimise” režiimis küsitava sisuga veebilehti [25].

Anonüümsus tähendab teenuste või süsteemide kasutamist oma tõelist identiteeti avaldamata. Veebisaitidele võib nähtav olla kasutaja tegevus, aga pole teada isik. Anonüümsus võib olla meetod teiste väärtuste (näiteks privaatsus või vabadus) realiseerimiseks. Veebisaite külastades ning rakendusi kasutades võib tunduda, et nendega ollakse otseühenduses, kuid tegelikult läbivad andmepaketid ka muid võrguseadmeid, kus neid salvestada ja analüüsida võidakse. Seejuures on kõigile vahepealsetele seadmetele nähtav ka kasutaja IP-aadress. Täpselt nagu kirja saatmiseks on vaja postiaadressi, on internetis andmepakettide edastamiseks vaja IP-aadressi. Seetõttu ei piisa anonüümseks sirvimiseks vaid oma seadmes muudatuste tegemisest, vaid on vaja saavutada eristamatus teistest.

Tor Browser

Lihtsaim ning levinum viis anonüümseks veebisirvimiseks on kasutada Tor Browserit[4]. See on Mozilla Firefox ESR-i[5] põhjal loodud brauser, mis üritab vähendada info lekkimist ning kasutab ühenduste loomiseks Tor vaheservereid.

Tor Browseris on paljud digitaalsõrmejäljena kasutatavad funktsioonid asendatud enamlevinud võltsväärtustega või välja lülitatud. Võrguliiklus saadetakse krüpteerituna läbi ülemaailmse tunneli, mis koosneb vaikimisi kolmest juhuslikult valitud sõlmest (serverist). Kõigil kasutajatel pole küll sama väljundsõlm ja IP-aadress, kuid võimalikke tunneli viimaseid sõlmi on alla tuhande[6]. Tor Projecti statistika kohaselt on Toril päevas umbes kaks miljonit kasutajat. Kuna iga veebisaidi jaoks vahetatakse tunneli servereid (v.a esimest), näivad veebisaitidele (ja vahepealsetele võrguseadmetele) kõik selle brauseri kasutajad ühesugustena. Neile on näha, et külastus pärineb Tori võrgust, kuid pole teada mis IP-aadressilt algne päring tehti. Siiski nõuab anonüümsuse säilitamine ka teatavat kasutusharjumuste muutmist. Näiteks pole soovitatav Tori kaudu sisse logida kasutajat identifitseerivatesse kontodesse. Kuigi teoreetiliselt on erinevaid veebisaidid ja vahelehed üksteisest eraldatud, ei saa selles kindel olla ning näiteks Facebooki sisselogimine võib aidata isikut tuvastada ka teistel saitidel.

[4] https://torproject.org/docs/
[5] https://www.mozilla.org/en-US/firefox/organizations/
[6] https://www.dan.me.uk/tornodes

Samuti tuleks vältida krüpteerimata (HTTP) veebisaite, kuna need on pahatahtliku väljundsõlme poolt muudetavad ning kogu nende sisu (sealhulgas sisestatud paroolid ja e-kirjad) on nähtav. See ei ole probleemiks ainult Tori kasutades, vaid kõigi veebibrauserite ning internetiühenduste korral.

Virtuaalne privaatvõrk

Kuigi Tor Browser pakub teiste veebibrauseritega võrreldes head kaitset jälituse, pealtkuulamise ning tsensuuri eest, pole see paljudele inimestele peamise brauserina sobilik. Kuna kogu võrguliiklus saadetakse läbi kolme sõlme, mis võivad asuda erinevates maailmajagudes, on see otseühendusest oluliselt aeglasem ning ei sobi ka suurte failide allalaadimiseks. Kui on soov varjata veebisaitide eest oma füüsilist asukohta või interneti teenusepakkuja eest kasutusharjumusi (külastatud veebisaite), võib parem valik olla virtuaalne privaatvõrk (ingl *virtual private* network) ehk VPN. Seda kasutades saadetakse liiklus samuti läbi turvalise tunneli, kuid selleks kasutatakse vaid üht vaheserverit. VPN-i kasutamine pakub Torist paremat valikut serveri omaduste ning turvalisuse üle. VPN-i teenust pakuvad ka näiteks koolid ja ettevõtted asutusesesisestele failidele või piiratud sisule mujalt turvalise ligipääsu lubamiseks. Lisaks leiab internetist sadu teenusepakkujaid, kelle servereid tasuta või väikse kuutasu (tavaliselt 2 kuni 10 eurot) eest kasutada saab. Suurematel teenusepakkujatel (näiteks ExpressVPN[7]) on tuhandeid servereid üle maailma, mis võimaldab teenuse kasutajatele suurt valikut veebisaitidele päringute tegemiseks kasutatava asukoha üle. Välismaise serveri kasutamine aitab vältida geoblokeeringut ning muid piiranguid, kuid mida kaugemal server asub, seda suurem on veebilatentsus (päringuteks kuluv aeg). Lähedalasuvate riikide servereid kasutades võib interneti kiirus väheneda väga vähe ning sama linna puhul jääda praktiliselt muutumatuks.

VPN-i kasutamine vähendab info lekkimise võimalust näiteks Wi-Fi võrke kasutades. See aitab ära hoida krüpteerimata sisu pealtkuulamise ja muutmise ning ka vahendusründed (ingl *man-in-the-middle attack*). Seda juhul kui VPN-i serverit usaldatakse, aga kasutatavat internetiühendust mitte. Turvalise krüpteeritud tunneli tõttu näeb internetiteenuse pakkuja suhtlust vaid VPN-i serveriga ja külastatud veebisaite enam tuvastada ei saa. Ilma VPN-i kasutamata omab ülevaadet interneti kasutusest näiteks Wi-Fi võrgu haldaja, kuid VPN-i kasutades näeb kogu võrguliiklust ja võib logiandmeid säilitada virtuaalse privaatvõrgu

[7] https://www.expressvpn.com/

server. Paljud teenusepakkujad väidavad, et nad ei salvesta klientide andmeid, kuid kindel ei saa selles kunagi olla [26].

2.2 Miks on vaja koolides õpetada infoturvet?

Kiiresti muutuvas maailmas on teadmised infoturbest vajalikud igale arvutikasutajale. Enamik inimestest ei mõtle arvutiturbest enne probleemide tekkimist, kuid siis on tavaliselt juba liiga hilja ning tekkinud kahju võib olla pöördumatu [27].

Viimaste kümnendite arengud on muutnud võimalikuks tervete inimgruppide ning rahvaste kommunikatsiooni seire. Lisaks suurenevad iga aastaga küberohud ning -intsidentide arv [28]. Kuigi operatsioonisüsteemide tootjad pakuvad kasutajatele sagedasi turvauuendusi ja sisseehitatud tööriistu turvalisuse suurendamiseks, on paljud neist vaikimisi välja lülitatud või kasutajate poolt teadmatu käitumisega kergesti õõnestatavad. Efektiivseks andmete kaitseks on vaja ka kasutajapoolset turvateadlikkust. Ohtude vältimiseks on oluline peamistest infoturbe probleemidest ülevaadet omada ning neid vajalikke tarkvarasid kasutades tuvastada ja ennetada osata, kuna kasutaja enda tegevus on suurim oht tema turvalisusele [29].

2.3 Olemasolevad õppematerjalid

Valikõppeaine „Küberkaitse“

Eesti NATO Ühingu, Tallinna Tehnikaülikooli, Eesti Informaatikaõpetajate Seltsi ja Kehtna Kutsehariduskeskuse koostööprojektis loodi Küberkaitse ainekava materjal gümnaasiumile [30]. Projekti toetas Haridus- ja Teadusministeerium ning selle tulemusena valmis Tallinna Ülikooli Pressbooks'i keskkonda e-õpik[8].

Õpiku põhjal läbiviidav baaskursus "Infoühiskond ja isiklik turvalisus" on mõeldud gümnaasiumi- ning kutsekooliõpilastele, kellelt ei eeldata küberkaitse erialateadmisi. Õpik jaguneb kolmeks plokiks: "Infoühiskond", "Risk ja oht", ning "Edasiõppimine ja karjäär", mis sisaldavad kokku kuutteist peatükki.

Lõputöö raames loodav õppematerjal erineb "Küberkaitse" õppeainest igapäevaselt tavakasutajaid puudutavatele probleemidele ning praktilisematele ja konkreetsematele ülesannetele keskendumisega. Paljud "Küberkaitse" õpiku ülesanded nõuavad testide täitmist, veebilehtede uurimist või kirjutamist, mille käigus tuleb teooria põhjal avaldada oma arvamust. Samuti on tundides käsitletavad teemad üksteised üsna erinevad ja suures osas

[8] https://web.htk.tlu.ee/digitaru/kyberkaitse

mittetehnilised. Praktilisi infoturbe teadmisi ning rakendustarkvara kasutamist õpetatakse võrdlemisi väikses mahus. Sellest tulenevalt pole kattuvus loodava õppematerjaliga suur, kuna lõputööna loodavas kursuses keskendutakse just praktilistele ülesannetele ehk rakendustarkvara ning süsteemiprogrammide kasutamisele. Lisaks ei käsitleta valmivas kursuses mittetehnilisi teemasid ning ülesanded on seetõttu konkreetsemad ning ei nõua õpilastelt palju enda arvamuse avaldamist.

Targalt Internetis

Targalt Internetis on projekt, mille "missioon on laste ja lapsevanemate targem internetikasutus ning laste seksuaalset ärakasutamist esitava sisuga materjalide leviku tõkestamine internetis"[9]. Selle raames on koostatud ka koolitus- ja teavitusmaterjale lastele, õpetajatele ning lapsevanematele. Õppematerjalid ei moodusta ühte tervikut, vaid mitu eraldiseisvat osa. Lõputööna loodava kursusega kattuvad osaliselt õpetajatele iseseisvaks õppimiseks suunatud materjalid. Neist loodava kursusega kõige sarnasemad on "Nutiseadmete turvalisus"[10], "Erinevad autentimisviisid"[11] ning "Kus on minu andmed"[12]. Materjalides õpetatud teooria langeb suures osas kokku loodava kursuse eesmärkide ja põhimõtetega, kuid kolme teema maht on kokku vaid kuus akadeemilist tundi (vastavalt 3, 2 ja 1).

Tartu Ülikooli infoturbe aine

Tartu Ülikoolis on 2013. aastast õpetatud 3 EAP (1 EAP = 26 tundi) väärilist ainet "Infoturve (MTAT.07.028)"[13]. See on mitteinformaatikutele suunatud sissejuhatav kursus, mis annab ülevaate infoturbest ja sellega seonduvatest probleemidest.

Kuid selle kursuse teemad on eelteadmisteta gümnaasiumiõpilastele tehniliselt liiga keerulised ning teoreetilised. Kuigi tulevased õpetajad saavad selle aine läbida, on gümnaasiumis infoturbe õpetamiseks vajadus praktiliste ning paindlike ülesannete järele, mis oleks õpilastele võimetekohased ning aktuaalsed.

2.4 Õppematerjali vajadus

Infoturve on tehniliselt väga keeruline valdkond, mille teoreetilise õpetamise jaoks jääb ühe gümnaasiumikursuse maht selgelt liiga väikseks. Samas kasutavad arvuteid ja nutiseadmeid

[9] https://www.targaltinternetis.ee/projektist/
[10] https://sisu.ut.ee/nutiturva
[11] https://sisu.ut.ee/autentimine
[12] https://sisu.ut.ee/minuandmed
[13] https://courses.cs.ut.ee/2019/infsec/spring

suur enamus inimestest ja valdkonna teadmised on ohtude, piinlikkuse ning salajaste andmete lekkimise vältimiseks väga olulised.

Viimase kümne aastaga on loodud palju rakendusprogramme, mis pakuvad kaasaegseid tipptasemel turbefunktsioone, kuid on samas lihtsasti kasutatavad. Varasemalt ainult ekspertidele mõistetav keerukus on neis asendatud mõistlike vaikesätete ja lihtsustatud kasutuskogemusega, mis ei eelda valdkonnateadmisi ning arusaamist taustal toimuvast. Näiteks ei vaja nutiseadmetes suhtluse otspunktkrüpteerimine võtmete loomist ning haldamist ja paljude muude valikute tegemist. Rakendused Signal, WhatsApp ning Facebook Messenger kasutavad otspunktkrüpteerimist automaatselt või võimaldavad lihtsat aktiveerimist. Õppematerjalis selgitatakse, miks ei saa teenusepakkujate ning tootjate lubadusi alati uskuda. Samas tähendab avatud lähtekoodiga usaldusväärsete alternatiivide olemasolu, et infoturvet saab nüüd suurepäraselt rakendada ja õppida ka oluliselt praktilisemalt, ainult mõningaid taustteadmisi käsitledes.

Arvuteid kasutatakse väga erinevatel eesmärkidel ning ka inimeste privaatsusvajadused on erinevad. Seetõttu võimaldab suure hulga rakendusprogrammide kasutamine ning operatsioonisüsteemide seadistamise tutvustamine igal õpilasel talle huvipakkuvamate lahendustega täpsemalt tutvuda. Suureneb ka tõenäosus, et midagi õpetatust väljaspool kursust oma seadmes igapäevasesse kasutusse võetakse ja seeläbi infoturbest rohkem huvitutakse.

Teoreetilise infoturbe teadmisi on küll kasulik omada, kuid väljaspool õppeainet algtasemel teooriat enamasti rakendada ei saa. Nende õpetamisel gümnaasiumiõpilastele jäävad piiratud aja ning eelteadmiste puudumise tõttu käsitlused üsna pinnapealseks. Privaatsusprogrammid või seadistused võivad seevastu oluliselt vähendada kasutaja andmete automaatse saatmise ning lekkivate andmete hulka.

3. Metoodika

Selles peatükis antakse ülevaade õppematerjalide loomise protsessist ning põhjendatakse tehtud valikuid. Lisaks kirjeldatakse informaatikaõpetajatele suunatud konverentsil läbi viidud töötuba.

3.1 Materjalide kogumine ja süstematiseerimine

Selle bakalaureusetöö raames loodud kursus ja kasutatavad ideed põhinevad valdavalt ingliskeelsetel e-raamatutel ning õpikutel. Peamise allikana kasutati O'Reilly[14] (varasemalt Safari Books Online) digitaalraamatukogu, mis pakub ligipääsu tehnoloogia- ning äriteemalistele raamatule ning videokursustele, millest umbes 500 on turvalisuse teemal. Lisaks kasutati Eesti raamatukogusid, välismaa raamatukogude poolt pakutavat Rakuten OverDrive'i[15] ning heliraamatute kuulamiseks Audible't[16]. Kasulikku taustinformatsiooni ning uudiseid saadi ka taskuhäälingutest, kuid otseselt allikana neid ei kasutatud.

Rõhuv osa turbeteemalisest kirjandusest on suunatud ettevõtete ja organisatsioonide infoturbetöötajatele ning ülikooliõpikud on teoreetilise suunitlusega kursuste jaoks. Konkreetseid soovitusi tavakasutajale isikliku arvuti seadistamiseks ning tarkvara kasutamiseks jagatakse harva. Osalt arvatavasti seetõttu, et mitmesajalehelise raamatu kirjutamine ja kirjastamine on pikk protsess ning lisaks võib ka müük kesta aastaid, kuid internetis toimuvad muutused väga kiirelt. Mitu kuud varem antud soovitused ei pruugi lugemise hetkel enam täielikult päevakohased olla ning autorid eelistavad teemasid, mis ajas vähem muutuvad.

Lõputöö raames läbi vaadatud raamatutest osutus selle kursuse eesmärgiga kõige samalaadsemaks 2017. aastal välja antud 302-leheküljeline "Digital Privacy and Security Using Windows: A Practical Guide".

Infoturbe valdkonna omapäraks on see, et veebilehtedelt ning internetifoorumitest leiab rohkem konkreetseid soovitusi kui raamatutest. Aga kui õpikute autoritel on tihti doktorikraad või mitukümmend aastat töökogemust ning mitu inimest kontrollib enne kirjastamist teksti üle, võib internetis sisu ja arvamust avaldada igaüks. Siiski leidub veebisaite, mille aruteludes peetakse lugu tehnilisest korrektsusest.

Üks suurimaid privaatsusele suunatud kogukonna poolt loodud veebisaitidest on Privacy Tools[17]. Sealt võib lisaks viidatud juhenditele ning informatsioonile leida kategooriatesse organiseeritud tarkvarasoovitusi. Veebisaidil avaldatava sisu üle arutletakse GitHubis ning Redditis[18]. Sealsed soovitused sisaldavad ainult avatud lähtekoodiga tarkvara, mis

[14] https://www.oreilly.com/
[15] https://www.overdrive.com/
[16] https://www.audible.com/
[17] https://privacytools.io
[18] https://www.reddit.com/r/privacytoolsIO/

privaatsuspoliitka kohaselt lubavad säilitada kasutajate privaatsuse. Ka loodava kursuse materjalid põhinevad osaliselt sealsetel soovitustel.

3.2 Rakendustarkvara valimise metoodika

Suur osa kursuse jaoks loodud ülesannetest tutvustavad ning õpetavad mõne rakendusprogrammi kasutamist. Võimaluse korral eelistati operatsioonisüsteemi sisseehitatud (turbe)funktsioone ja utiliite, kuid paljude printsiipide praktiliselt tutvustamine vajab täiendava tarkvara allalaadimist. Kuna tegu on infoturbe kursusega oli nende valikul määravaks minimaalne andmete kogumine, regulaarsed uuendused ning selge ja mõistlik privaatsuspoliitika.

Avatud lähtekoodiga tarkvara

Õppematerjalide praktilistes ülesannetes eelistati olemasolu korral avatud lähtekoodiga tarkvara kasutamist.

Lähtekoodtarkvara ehk avatud lähtekoodiga tarkvara puhul avalikustatakse lisaks täitmisfailidele ka selle lähtekood. Avaliku lähtekoodi olemasolul saavad sõltumatud eksperdid kontrollida turvadefektide ning tagauste puudumist. Tagauks on salajane või dokumenteerimata viis, mis võimaldab asjakohase volituseta ning kaitsevahenditest möödudes saada juurdepääsu süsteemile [5].

Krüpteerimise korral tähendab see näiteks, et lisaks paroolile või võtmele eksisteerib kasutaja teadmata neid mittevajav meetod failide või sõnumite dekrüpteerimiseks. Turbeprogrammide puhul võib tagaukse olemasolu nurjata nende kasutamise eesmärgi. Väljaspool entusiastidele suunatud Linuxi distributiive (ingl *distribution*) (eelkõige Gentoo Linux ja Arch Linux) on kasutajate poolt programmide lähtekoodist kompileerimine vähelevinud. Kuigi leidub võimalus, et allalaadimiseks pakutav täitmisfail ei pärine lähtekoodist, on see siiski vähetõenäoline. Teine võimalus täitmisfailide usaldusväärsuse tõestamiseks on reprodutseeritavate ehk korratavate ehitusinstrumentide (programm täitmiskõlbuliku rakenduse loomiseks lähtekoodist) kasutamine. Nende puhul saadakse erinevates seadmetes ning keskkondades kompileerimisel täpselt sama tulemus. See võimaldab tõestada, et kasutati muutmata kujul lähtekoodi. Sellist kompileerimisviisi kasutavad muuhulgas Tor[19], Bitcoin ning osaliselt Linuxi distributiiv Debian.

[19] https://blog.torproject.org/deterministic-builds-part-two-technical-details

Kuigi teoreetiliselt on võimalik kõiki programme pöördkonstrueerimise abil analüüsida, on saadud koodi mõistmine ja analüüsimine nii keeruline, et osutub vähegi suuremate projektide puhul praktiliselt võimatuks. Seetõttu tuleb omandtarkvara kasutamisel ning paigaldamisel selle autoreid ja allikat pimesi usaldada. Edward Snowdeni lekitatud dokumentide põhjal saavad USA luureagentuurid sundida riigis tegutsevaid firmasid andmeid koguma ning edastama. Seejuures ollakse kohustatud seda üldsuse eest varjama ning ajakirjanikele valetama [15].

Vabatarkvara (vabadus kasutada ja suvaliselt muuta) kogukondade (näiteks KDE[20]) puhul kommertseesmärke ja kindlaid omanikke ei ole, mistõttu vajadus kasutajate andmeid koguda praktiliselt puudub. Kõigil kasutajatel muudatuste tegemist lubava litsentsi tõttu see ka ei õnnestuks - kergelt ja seaduslikult saab luua haruversiooni (ingl *fork*), millest kasutajale mittesobivad funktsioonid on eemaldatud.

Nutiseadmete tarkvara

Õppematerjalides käsitletakse väikses mahus ka nutiseadmete turvamist. Mobiil-operatsioonisüsteemide piiratud seadistusvõimaluste, rohkete sensorite ning rakendustele antavate õiguste tõttu on nutiseadmete kasutamisel privaatsuse ja turvalisuse säilitamine keerulisem.

Nutiseadmetes on ka avatud lähtekood vähemlevinud. Kuigi Android on avatud lähtekoodiga, sisaldavad peaaegu kõik müüdavad seadmed tootjapoolsete muudatuste ja Google Play poe näol ka omandtarkvara. Suurim avatud lähtekoodiga Androidi distributiiv on LineageOS[21], mis on paigaldatav 21 tootja valitud seadmetele. Lisaks on saadaval ainult tasuta ja avatud lähtekoodiga rakendustest koosnev rakendustepood F-Droid[22]. Aurora Store (paigaldatav F-Droidist) võimaldab Google Play poest rakenduste paigaldamist Google'ile seadme üle kontrolli (juurkasutaja õigusi) andmata. LineageOS on siiski vähelevinud (1,53 miljonit kasutajat[23]) ning seadme tarkvara asendamine muudab paljudel juhtudel garantii kehtetuks.

Apple'i iOS on oluliselt piiratum ning sarnaseid võimalusi ei paku. See eest on iOS vaikimisi Androidist oluliselt privaatsussõbralikum, kuna Apple ei ole reklaamifirma ning ei vaja seetõttu suurel hulgal kasutajate andmete kogumist. iOS-i peetakse populaarsetest

[20] https://kde.org/community/whatiskde/
[21] https://lineageos.org/
[22] https://f-droid.org
[23] https://stats.lineageos.org/

operatsioonisüsteemidest kõige turvalisemaks ning uute turvaaukude (*remote jailbreak*) avastamise ning müümise eest on sellest huvitatud osapooled (näiteks Zerodium[24]) nõus maksma üle miljoni euro. Seni tuntuim iOS-i turvaauke ära kasutav nuhkvara on Iisraelis NSO Groupi poolt loodud Pegasus, mis võimaldas pärast seadmes (sõnumiga saadetud) lingi avamist või WhatsAppi kõne tegemist lugeda selle sõnumeid, jälgida kõnesid, koguda paroole ning informatsiooni rakendustest (muuhulgas iMessage, Facebook, Skype) [31]. Apple osales ka eelnevalt kirjeldatud PRISM programmis ja on kohustatud järgima USA riigiorganite ettekirjutusi, mistõttu ei saa firma avalikult antud lubadustes ka iPhone'ide puhul kindel olla.

Nutiseadmete virtualiseerimine on Windowsist ja Linuxist oluliselt keerulisem. Seetõttu tuleb ülesandeid lahendada isiklikus või kooli nutiseadmes. Ei saa eeldada, et õpilased soovivad oma seadmesse täiendavat tarkvara paigaldada. Seepärast on loodud õppematerjalides nutiseadmete puhul piirdutud sisseehitatud funktsioonide kasutamise ning seadistamisega.

3.3 Õppematerjalide loomise keskkond

Õppematerjalide[25] loomiseks kasutati Tartu Ülikooli arvutiteaduse instituudi kursuste keskkonda[26], mille aluseks on vikitarkvara PmWiki[27]. See on sisuhaldussüsteem, mis võimaldab luua ja muuta veebilehti HTML-i ja CSS-i kasutamata. Selle asemel on redigeerimiseks kasutusel märgendkeel, mille süntaks on teiste laialtlevinud märgendkeelte Markdown (kasutusel Redditis, GitHubis ja Stack Exchange'is) ja Vikipeediates kasutatava Wikitextiga võrreldes unikaalne ning ei võimalda adekvaatesitust (WYSIWYG) [32]. Reeglid on siiski üsna lihtsad ja võimaldavad lühidalt teksti vormindada ja pilte ning videoid lisada (vt Joonis 1).

Editing Main.Infoturbest

```
!Infoturbest
* [[https://et.wikipedia.org/wiki/Infoturve|Infoturve - Vikipeedia]]
* [[https://en.wikipedia.org/wiki/Information_security|Information security - Wikipedia]]
!!Põhiterminid
%rfloat width=300% Attach:infoturbeeesmärgid.png %%
:Infoturve:Teabe ning infosüsteemide kaitsmise protsess, mille eesmärk on tagada andmete
käideldavus, konfidentsiaalsus ning terviklus.
```

Joonis 1. Näide vikisse andmete lisamisest

[24] https://zerodium.com/program.html
[25] https://courses.cs.ut.ee/t/infoturvekoolis
[26] https://courses.cs.ut.ee
[27] https://www.pmwiki.org/wiki

3.4 Töötuba informaatika õpetamise konverentsil

Bakalaureusetöö raames viidi 7. veebruaril "Informaatika õpetamise konverents 2019" raames läbi 55-minutiline töötuba "Praktiline infoturve – privaatsus internetis". Konverents[28] oli suunatud erinevate kooliastmete (sealhulgas koolieelsete õppeasutuste ja kõrgkoolide) õpetajatele ning nelja päeva jooksul toimusid ettekanded, töötoad ja arutelud erinevatel teemadel.

Enne konverentsile töötoa registreerimist toimus arutelu töö juhendajatega potentsiaalsete ülesannete teema üle. Jõudsime otsusele, et selleks saab kas privaatsus või autentimine. Kuigi oli soov käsitleda mõlemat teemat, leidsime ülesannete valmimise ning läbilahendamise järel, et ajapiirangu tõttu see võimalik pole.

Töötuba viidi läbi konverentsi esimesel päeval koostöös lõputöö juhendajaga ja see koosnes 20-minutiliseest sissejuhatusest teemasse ning 30-minutilisest praktilisest osast. Sissejuhatuses tutvustati osalejatele praktilise infoturbe vajadust, kursuse loomise tausta ning esialgset kava. Praktilises osas jagati töötoas osalejatele töölehed (seitse A4-formaadis lehte), mille lahendamist koos alustati. Töölehed on leitavad lisast I. Ülesannete eesmärk oli kasutaja arvutis Mozilla Firefoxi veebibrauseri privaatsemaks seadistamine. Esmalt tutvustati vaikesätetega brauserite poolt külastavatele veebilehtedele saadetavaid andmeid ning seejärel alustati seadete muutmist ning privaatsuslaienduste paigaldamist. Töö käigus toimus elav arutelu ning osalejad said vastuse oma küsimustele. Pärast töötuba vastasid osalejad tagasisideküsimustikule, mille leiab lisast II.

4. Tulemused

Selles peatükis antakse ülevaade kursuse "Praktiline infoturve" loomise tulemustest. Kursuse materjal on kättesaadav Tartu Ülikooli arvutiteadus instituudi kursuste veebisaidil[29].

4.1 Eesmärk ja õpiväljundid

Lõputöö eesmärgiks oli koostada kursus ja ülesannetega õppematerjalid gümnaasiumis infoturbe õpetamiseks ning tulevaste õpetajate ettevalmistamiseks. Kursuse käigus antakse ülevaade peamistest turvariskidest kasutajate seadmetele ning failidele.

[28] https://didaktika.cs.ut.ee/konverents2019/
[29] https://courses.cs.ut.ee/t/infoturvekoolis

Kursuse eesmärk on veenda õpilasi infoturbe olulisuses. Selle abil loodetakse vähendada ebaturvalisi kasutusharjumusi nagu nõrgad paroolid ja nende korduvkasutamine. Kursuse teemad ja ülesanded on valitud selliselt, et nende rakendamisest võiks õpilastele kasu olla ka väljaspool kursust.

Kursuse läbinud õpilane omab algteadmisi infoturbest ning oskab rakendada turvameetmeid kaitseks enamlevinud infoturvariskide vastu.

4.2 Koostatud kursus ja õppematerjal

Valminud õppematerjal koosneb kahest plokist - "Infoturbest" ja "Operatsioonisüsteemid". Esimeses käsitletakse infoturvet üldisemalt ning platvormideüleselt ning teises konkreetseid operatsioonisüsteeme (Windows 10 ning Ubuntu 18.04) ja nutiseadmeid. Mõlemad plokid koosnevad omakorda seitsmest topelttunnist ning plokki sissejuhatavast teoreetilisemast materjalist (vt Joonis 2).

Iga tund algab teoreetilise sissejuhatusega ning tausta ja olulisuse selgitusega. Sellele järgnevad kordamisküsimused, mis nõuavad enamasti täiendavate (lingitud) materjalide lugemist.

Joonis 2. Valminud õppematerjalide sisukord

Mõned ülesanded vajavad virtualiseerimise (Oracle VM VirtualBox[30]) kasutamist ning Windowsi puhul Pro või organisatsioonilist (Education ja Enterprise) väljaannet.

Esimese ploki praktiliste ülesannete käigus õpitakse informatsiooni kaitsma ning oma teabe tahtmatut levikut vähendama. Käsitletakse turvalisi ning privaatseid failiedastusviise ja võimalikest andmeleketest tekkiva kahju minimeerimist. Tutvustatakse avatud lähtekoodiga alternatiive omandtarkvarale ning privaatsussõbralikumaid alternatiive populaarsetele veebiteenustele.

Teises plokis õpitakse turvama oma arvutit, nutiseadet ja internetiühendust. Käsitletakse Windowsi sisseehitatud turbefunktsioone ning tööriistu ning vähendatakse telemeetria saatmist Microsoftile privaatsussätete muutmisega. Tutvutakse operatsioonisüsteemi poolt seadmesse salvestatava tegevuslogi ning -jälgede uurimise ning kustutamisega. Selgitatakse tulemüüride, domeeninimede süsteemi ning virtuaalse

[30] https://www.virtualbox.org/

privaatvõrgu kasutamist. Virtuaalmasina abil tutvutakse Linuxi (Ubuntu) operatsioonisüsteemi ning selle käsureaga. Ubuntu[31] valiti selle pika kestustoe (ingl *long-term support*) tõttu, mis võimaldab loodud virtuaalmasinale veel mitu aastat turvauuendusi paigaldada. Tutvustatakse ka Bitdefender Total Security tarkvara, mis koondab ühte programmi mitmed kursuse jooksul tutvustatud teemad ja funktsioonid, kuid on pärast prooviperioodi tasuline ja pole avatud lähtekoodiga. Tarkvara valikul on üldiselt lähtutud selle populaarsusest privaatsust ning turvalisust hindavate inimeste hulgas ja regulaarsetest uuendustest. Süsteemitarkvara kasutamise ülesannete valik põhineb potentsiaalsete nõrkuste eemaldamisel ning riskide maandamisel.

Näide valminud materjalist – Windowsi haldamine

Kuna õppematerjalide maht on lõputöösse lisamiseks liiga pikk, on need leitavad aadressilt https://courses.cs.ut.ee/t/infoturvekoolis.

Järgnevalt on näitena kirjeldatud ühe topelttunni materjale. Selleks on teise ploki, „Operatsioonisüsteemid“, esimene tund – 2.1 Windowsi haldamine.

Tunni alguses tutvustatakse peamiseid Windowsi seadistamise tööriistu – juhtpaneel (ingl *Control Panel*) ning Sätted.

Selle topelttunni jooksul lahendatakse kuus ülesannet:

- **Windowsi privaatsussätete muutmine** – Windowsi telemeetria tutvustamine ja arvutite seadistamine väiksemamahuliseks andmete kogumiseks ning Microsoftile saatmiseks.
- **W10Privacy**[32] – Tööriist täiendavate privaatsusseadmete muutmiseks. Kasutatakse virtuaalmasinas, et vältida võimalike probleemide tekkimist õpilaste seadmetes. Programm võimaldab kasutajatel märkeruutude abil muuta sadu sätteid ning eemaldada või keelata Windowsi sisseehitatud rakenduss, mis tavasätetest võimalik pole.
- **Seadmest ebavajaliku tarkvara eemaldamine** - Iga arvutisse paigaldatud programm on potentsiaalne turvarisk. Seetõttu peaks paigaldatud olema vaid vajaminevad programmid. Ülesande käigus tutvustatakse rakenduste desinstallimist, kuid hoiatatakse liigse kustutamise eest.

[31] https://ubuntu.com
[32] https://www.winprivacy.de/english-home/

- **Tarkvara automaatne uuendamine Ninite abil** – Paljud Windowsi programmid ei võimalda automaatset uuendamist - uue versiooni paigaldamine vajab paigaldusfaili alla laadimist ning korduvalt paigaldusprotsessi läbiviimist. Ninite[33] võimaldab tarkvara paigaldamist ning uuendamist automatiseerida. Märgitud tarkvara paigaldatakse taustal automaatselt mõistlike sätete ning ilma täiendava rämpsvarata. See võimaldab vähese vaevaga kõiki seadmes olevaid programme uuendatuna hoida.
- **Turvalogi uurimine** – Windowsi Event Vieweri kasutamine logide uurimiseks. Tutvutakse logidesse salvestavate sündmusetüüpide ning tasemetega. Õpilased saavad seejärel kontrollida, kas keegi on nende eemaloleku ajal seadmesse sisse loginud või seda ebaõnnestunult teha püüdnud.
- **BleachBit**[34] – avatud lähtekoodiga programm arvutist ebavajalike andmete kustutamiseks ning andmete hävitamiseks. Võimaldab kustutada tuhandete programmide kasutusjälgi ning muid faile, mille olemasolust kasutaja tõenäoliselt teadlik pole.

4.3 Töötuba

Lõputöö osana viidi 7. veebruaril "Informaatika õpetamise konverents 2019" raames Tartu Ülikooli J. Liivi 2 õppehoones läbi töötuba. Töötuppa registreerus enam kui kakskümmend konverentsil osalenud õpetajat. Lisaks töölehtedele kasutati terve töötoa vältel sülearvutiga ühendatud projektorit – esmalt esitluseks ning seejärel üheskoos töölehe ülesannete lahendamiseks ning selgituste andmiseks.

Töötoa materjalid

Töötoa praktiliseks osaks valmis seitsmest A4-st koosnev tööjuhend. Ülesannete lahendamine nõudis sülearvuti või Androidiga seadme olemasolu ning Mozilla Firefoxi kasutamist. Peaaegu kõigil osalejatel oli see kaasas ning vajadusel leiti paariline, kellega ülesandeid koos lahendada.

Esimese ülesandena külastati Panopticlick[35] ning Device Info[36] veebisaite, et tutvuda brauseri poolt taustal saadetava info hulga ning seda ära kasutavate jälitusmeetoditega. Seejärel asuti saadetavat andmehulka vähendama brauseri konfiguratsiooni muutmise (aadressiribal

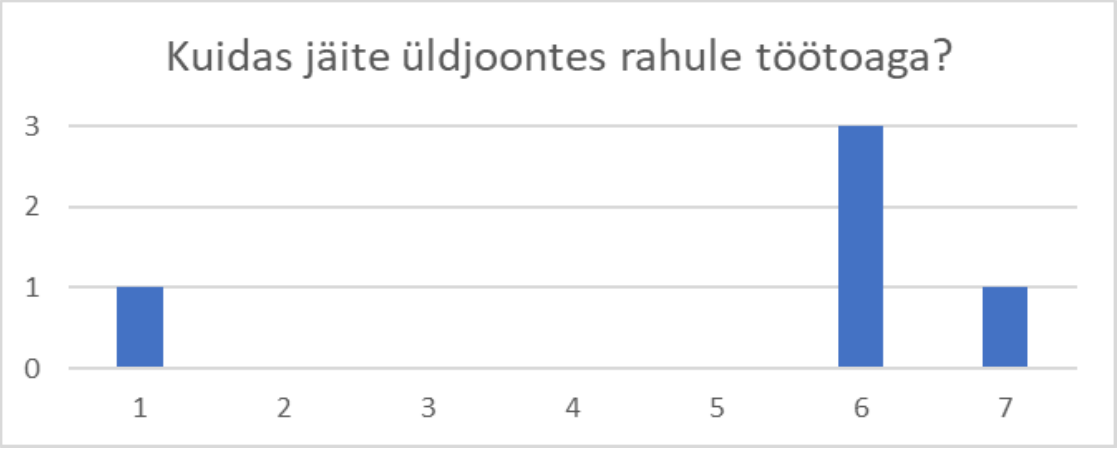
[33] https://ninite.com/
[34] https://www.bleachbit.org/
[35] https://panopticlick.eff.org/
[36] https://www.deviceinfo.me/

about:config sisestamisega) ning laienduste[37] paigaldamisega. Lõpetuseks tutvustati otsingumootreid Startpage ja DuckDuckGo privaatsemalt otsingute tegemiseks.

Brauserilaiendustena paigaldati Cookie Autodelete, uBlock Origin, Privacy Badger ning Decentraleyes ning täiendavalt muudeti üheteistkümne eelistuse väärtust. Kuna nii eelistusi kui laiendusi on tuhandeid ja ajapiirangu tõttu ei olnud võimalus kõike soovitut käsitleda, oli tehtud valik subjektiivne, kuid siiski peamisi privaatsusprobleeme kattev. Täieliku privaatsuse või anonüümsuse saavutamine polnud töötoa eesmärk. Kuigi tehtud muudatused vähendasid saadetavaid andmeid, võib see mõnes aspektis tähendada ka unikaalsuse suurenemist, sest valdav osa inimesi kasutab vaikesätteid. Kuna tehtud muudatused blokeerivad veebilehtede sisu ja muud taustal toimuvat (eelkõige uBlock Origin), võivad mõned veebisaidid funktsionaalsust kaotada. Kuid saadud kasu suurenenud privaatsusest ning blokeeritud tüütustest (reklaamid ja küpsiseteatised) kaalub üles võimalikud harvaesinevad probleemid. Lihtsaimaks lahenduseks probleemide tekkimisel on seadmesse teise veebibrauseri paigaldamine ning vajadusel selle kasutamine.

Töötoa tagasiside

Töötoas lõpus palusime kõigilt osalejatelt Google'i vormide kaudu tagasisidet. Mainisime selle olulisust lõputöö jaoks ja pakkusime ka võimalust seda hiljem esitada, kuid saime ainult viis vastust. Tagasiside vorm koosnes neljast küsimusest. Esimesed kaks olid kohustuslikud ning nõudsid skaalal valikute tegemist ja ülejäänud kaks tekstiväljad valikuliste soovituste ning kommentaaride sisestamiseks. Esmalt küsisime osalejatelt kuidas nad töötoaga rahule jäid skaalal ühest seitsmeni (vt Joonis 3).



Joonis 3. Osalejate tagasiside töötoale

[37] https://addons.mozilla.org/firefox/

Lisaks küsisime osalejatelt arvamust kursuses õpetatavate teemade olulisuse üle. Valikus oli kaheksa teemat – privaatsusprobleemid, autentimine, nutiseadmete turvalisus, Windowsi haldamine ja turvamine, ID-kaart, Wi-Fi võrgud, Linux ja torrentid ning täitmisfailid. Iga teema puhul tuli avaldada arvamust selle olulisuse üle skaalal ühest viieni.

Vastajad pidasid kõige olulisemaks autentimise ning nutiseadmete turvalisuse teemasid – mõlema puhul märkisid kolm vastajat olulisuseks „5“ ning kaks „4“. Kõige vastuolulisemaks osutus Linux, mille puhul kaks vastajat märkisid olulisuseks „1“, kaks vastajat „4“ ning üks „5“. Kõik ankeedi küsimused ning vastused on leitavad lisast II.

4.4 Arutelu

Esialgselt oli kavas luua ka kolmas plokk: “Edasijõudnutele”, kuid selles käsitletavaid teemasid pole veel valitud. Seetõttu jääb tulevikuks võimalus kursuse materjale täiustada ning uusi teemasid lisada. Lisaks tuleks ülesanded praktiliselt koolis läbi proovida – hinnata nende raskusastet, olulisust ning lahendamiseks kuluvat aega. Paljusid ülesandeid on lõputöö juhendaja ja informaatikaõpetajate koolituste läbiviija juba katsetanud. Lisaks kasutati „Autentimise“ ja „Nutiseadmete turvalisuse“ peatükkide ülesandeid erinevate ainete õpetajatele mõeldud aines „Digiohutus koolis“.

Lõputöö raames keskenduti ülesannete loomisele, kuid õpilastele kursuse läbi viimiseks võib tarvilik olla ka teoreetilise teksti täiendamine. Näiteks jääb võimalus tekstile lisada kontrollivaid interaktiivseid vaheküsimusi ning selgitada põhjalikumalt ülesannete teoreetilist tausta.

Kuna infoturbe valdkond ning ohud muutuvad väga kiiresti tuleb õpetajatel teemade ajakohasust hinnata ning vajadusel muudatusi teha. Seetõttu tuleks kaaluda tegevõpetajatele infoturbe õpetajakoolituste tegemist.

5. Kokkuvõte

Lõputöö eesmärgiks oli luua praktiline ülesandekogu ning õppematerjalid infoturbe teemalise gümnaasiumiastme valikkursuse jaoks. Tartu Ülikooli vikipõhisesse Courses keskkonda valmis neljateistkümnest akadeemilisest topelttunnist (90 minutit) koosnev õppematerjal, mis jaguneb kaheks plokiks: “Infoturbest” ja “Operatsioonisüsteemid”. Tundides on peamine rõhk praktilistel ülesannetel, milleks on enamasti rakendustarkvarade kasutama õppimine ning operatsioonisüsteemide seadistamine. Tundides käsitletavad teemad põhinevad reaalsetel ning aktuaalsetel infoturbe probleemidel. Kursuse eesmärk on osalt ka õpilastes infoturbe vastu huvi tekitada.

Lõputöö esimeses peatükis kirjeldatakse infoturvet üldiselt ning selle olulisust. Kirjeldatakse gümnaasiumis infoturbe õpetamise vajadust ning antakse ülevaade olemasolevatest eestikeelsetest valdkonna õppematerjalidest.

Teises peatükis kirjeldatakse õppematerjalide ning ülesannete loomise metoodikat ja põhimõtteid ning põhjendatakse neid. Kirjeldatakse rakendustarkvara valimise põhimõtteid ning antakse ülevaade materjalidel loomiseks kasutatud vikikeskkonnast PmWiki.

Kolmandas peatükis antakse ülevaade valminud õppematerjalidest ning selle õpiväljunditest. Samuti kirjeldatakse lõputöö raames õpetajatele suunatud konverentsil läbi viidud 55-minutilist töötuba „Praktiline infoturve – privaatsus internetis“, mille käigus õpetati osalejaid Mozilla Firefoxi veebibrauserit privaatsemaks seadistama ning tutvustati nelja privaatsuslaiendust.

Valminud materjale saab kasutada Tartu Ülikooli õpetajakoolituse raames ning see annab ka võimaluse testimaks ülesannete keerukust ja mahtu.

6. Viidatud kirjandus

[1] U.S. Code, Title 44, Chapter 35, Subchapter III, § 3542. US Law. Legal Information Institute, *Cornell Law School*. https://www.law.cornell.edu/uscode/text/44/3542 (06.05.2019)

[2] Merkow M. S., Breithaupt J. Information Security: Principles and Practices, 2nd Ed. Indianapolis: Pearson. 2014.

[3] Andress J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, 2nd Ed. Oxford: Syngress. 2014.

[4] Berghel H., Schneier B. Bruce Schneier on Future Digital Threats. *IEEE Explore*, 2018. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8301137 (06.05.2019)

[5] AKIT – Andmekaitse ja infoturbe leksikon. https://akit.cyber.ee/

[6] Bing C., Lynch S. N. U.S. charges North Korean hacker in Sony, WannaCry cyberattacks. *Reuters*, 2018. https://www.reuters.com/article/us-cyber-northkoreasony/u-s-charges-north-korean-hacker-in-sony-wannacry-cyberattacksidUSKCN1LM20W (06.05.2019)

[7] Burgess M. North Korea's elite hackers are funding nukes with crypto raids. *WIRED UK*, 2019. https://www.wired.co.uk/article/north-korea-hackers-apt38cryptocurrency (06.05.2019)

[8] Zetter K. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown. 2014.

[9] Aitken R. Global Information Security Spending To Exceed $124B In 2019, Privacy Concerns Driving Demand. *Forbes*, 2019. https://www.forbes.com/sites/rogeraitken/2018/08/19/global-information-securityspending-to-exceed-124b-in-2019-privacy-concerns-driving-demand/ (06.05.2019)

[10] Cole E. Online Danger: How to Protect Yourself and Your Loved Ones From the Evil Side of the Internet. New York: Morgan James Publishing. 2018.

[11] Hassan N., Rami H. Digital Privacy and Security Using Windows: A Practical Guide. New York: Apress. 2017.

[12] Stallings W., Brown L. Computer Security: Principles and Practice, 3rd Ed. Harlow: Pearson. 2015.

[13] Kim D., Solomon M. G. Fundamentals of Information Systems Security, 3rd Ed. Burlington: Jones & Bartlett Learning. 2016.

[14] Andmekaitse ja netiprivaatsus – Teie Euroopa https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protectiononline-privacy/index_et.htm (06.05.2019)

[15] Greenwald G. No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. New York: Penguin Random House. 2014.

[16] Greenwald G. Why privacy matters. TEDGlobal, 2014. https://www.ted.com/talks/glenn_greenwald_why_privacy_matters (06.05.2019)

[17] Schneier B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Norton Company. 2015.

[18] Big tech faces competition and privacy concerns in Brussels - Europe's beef with GAFA. *The Economist*, 2019.

https://www.economist.com/briefing/2019/03/23/bigtech-faces-competition-and-privacy-concerns-in-brussels (06.05.2019)

[19] Libert T. Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites. *International Journal of Communication, 2015.* https://timlibert.me/pdf/Libert-2015-Exposing_Hidden_Web_on_Million_Sites.pdf (06.05.2019)

[20] Merzdovnik G., *et al*. Block Me If You Can: A Large-Scale Study of TrackerBlocking Tools. *SBA Research*, 2017. https://www.securitee.org/files/trackblock_eurosp2017.pdf (06.05.2019)

[21] Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs. 2019.

[22] Europe's GDPR offers privacy groups new ways to challenge adtech - Whose business is your data?. *The Economist*, 2019. https://www.economist.com/briefing/2019/03/23/europes-gdpr-offers-privacygroups-new-ways-to-challenge-adtech (06.05.2019)

[23] Whitman M. E., Mattord H. J. Principles of Information Security, 6th Ed. Boston: Cengage Learning. 2017.

[24] Soovituslik juhend Microsoft Windows 10 turvaliseks kasutamiseks riigisektoris. *Riigi Infosüsteemi Amet*, 2017. https://www.ria.ee/et/ametist/juhendid/windows-10riigisektoris.html (06.05.2019)

[25] Loshin P. Practical Anonymity: Hiding in Plain Sight Online. Waltham, Massachusetts: Syngress. 2013.

[26] Mitnick K. D., Robert V. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. New York: Little, Brown and Company. 2017.

[27] Madden M., Rainie L. Americans' Attitudes About Privacy, Security and Surveillance. *Pew Research Center*, 2015. https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-securityand-surveillance/ (06.05.2019)

[28] Insight Report - The Global Risks Report, 13th Ed. *World Economic Forum*, 2018.

http://www3.weforum.org/docs/WEF_GRR18_Report.pdf (06.05.2019)

[29] Miller J. A. People are (still) the biggest security risks. *CIO*, 2016.

https://www.cio.com/article/3047131/people-are-still-the-biggest-security-risks.html (06.05.2019)

[30] Lorenz B., *et al.* Küberkaitse ainekava materjal gümnaasiumile, 2018 https://web.htk.tlu.ee/digitaru/kyberkaitse/back-matter/appendix/ (06.05.2019)

[31] Brewster T. Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text. *Forbes*, 2016. https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-knowabout-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/ (06.05.2019)

[32] Basic PmWiki editing rules. *PmWiki*, 2019.

https://www.pmwiki.org/wiki/PmWiki/BasicEditing (06.05.2019)

Lisad

I. Informaatika õpetamise konverentsi töötoa tööleht

Tööleht on saadaval aadressil:

https://courses.cs.ut.ee/t/infoturvekoolis/uploads/Main/töötuba.pdf

II. Informaatika õpetamise konverentsi töötoa tagasiside

Tagasisideküsimustik on saadaval aadressil:

http://lingid.ee/turvalisuseteemad

Tagasiside vastused on saadaval aadressil:

https://tinyurl.com/privaatsusinternetis

III. Õppematerjalid

Koostatud õppematerjalid on saadaval aadressil:

https://courses.cs.ut.ee/t/infoturvekoolis

IV. Litsents

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, _____Omar Purik_____,

(*autori nimi*)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose

_____Praktiliste ülesannete koostamine gümnaasiumile teemal „Infoturve“ _____,

(lõputöö pealkiri)

mille juhendajad on _____Kristjan Krips ja Tauno Palts_____,

(juhendaja nimi)

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.

Omar Purik

07.11.2019