Tartu Ülikool

Sotsiaal- ja haridusteaduskond

Haridusteaduste instituut

Kutseõpetaja õppekava

Madli Valtenberg

KÜBERKAITSEALASTE ALGTEADMISTE ÕPPEMATERJALI KOOSTAMINE KUTSEKOOLI ÕPILASTELE

Bakalaureusetöö

Juhendaja: Jüri Ginter

Tartu 2018

Sisukord

Kasutatud lühendid ja mõisted

Andmete leke- sh infoleke, andmete konfidentsiaalsuse rikkumine

Digitaalne jalajälg- endast interneti võrgu kasutamisel mahajäetud teave

DigiTurvis– Digiturbe ja küberkaitsega seonduvad teemad ja õpitulemused Eesti üld-, kutse- ja kõrghariduse õppekavades.

HTTPS- turvaline veebileht

ID-kaart- isikutunnistus

Identiteedi vargus- teise isiku tähtsate isikuandmete kuritarvitamine, millest võib tekkida isikule nii materiaalne või moraalne kahju

Infoturve- infovarade (andmed, riistvara, tarkvara, side, infrastruktuuri ja personali) turvalisuse tagamine

Kaugligipääs - ligipääs IKT seadmele üle internetivõrgu, geograafiliselt teisest asukohast kasutades teist IKT vahendit.

Küberjulgeolek- hõlmab kõiki elektroonilise teabe, teabekandjate ning –teenustega seotud toiminguid mis mõjutavad küberruumi julgeolekut. Peamine eesmärk on vähendada küberruumi haavatavust, st ennetada küberrünnakuid ning taastada rünnakute korral võimalikult kiiresti infosüsteemide toimimine.

Küberruum - arvutitel ja arvutisüsteemidel põhinev digitaalne ruum, mis toetab tänapäevase infoühiskonna toimimist ja koosneb peamiselt Interneti poolt võimaldatud tegevuskeskkondadest ja igapäevaste toimingute lihtsustamiseks loodud digitaalsetest andmekogudest

Liides – kahe või enama seadme, arvutiprogrammi vaheline vahelüli (alamprogramm), mis hõlbustab nende koostööd.

Ründevektor- on lähenemisviis või meetod, mida kasutades pahalane saab ligipääsu rünnatavasse arvutisüsteemi või võrku.

Teenustõkestus rünne- on rünne mille puhul server, ruuter või muu internetiliiklust korraldav seade koormatakse üle suure hulga ping- päringutega. Kuna seadmetel on tavaliselt tööks kasutada vaid piiratud võimsus siis võib seade rivist välja. Lühidalt on teenus kasutaja jaoks ebameeldivalt aeglane või hoopis kättesaamatu.

Tulemüür- funktsionaalüksus, mis vahendab liiklust kahe arvutivõrgu vahel ja kaitseb volitamatujuurdepääsu eest, üht neist või mingit osa

VPN- virtuaalne privaatvõrk. Privaatvõrk, mis kasutab avalikku telekommunikatsiooni infrastruktuuri, säilitades samal ajal privaatsuse ja turvalisuse

Viirus teadlikkus- teadmised erinevatest viirustest, nende avastamise ja ennetamise kohta.

Viirustõrje- (antiviirus, viirusetõrjeprogramm, viirusetõrje tarkvara) tarkvaraline viiruste avastamise ja kõrvaldamise vahend

Sissejuhatus

Igapäevaselt puutuvad kõik inimesed kokku nutitelefonide, arvuti ja internetiga, kasutatakse sotsiaalmeediat, erinevaid keskkondi, laetakse üles pilte, avaldatakse endast erinevat informatsiooni, mis kõik jääb küberruumi. Küberruumis tegutsevad kurjategijaid, kes soovivad teiste arvelt kasu saada. Tänapäeval piisab ka vähestest teadmistest, et teha kahju kasutajatele, kes oma andmeid kaitsta ei oska.

Info- ja kommunikatsioonitehnoloogia areneb tänapäeval kiiresti, andmemahud kasvavad ja suureneb seadmete hulk, mis ühendatakse andmesidevõrkudesse ning mis omavad suurt mõju nii igapäevaelu, majanduse kui ka riigi toimimisele. Võimalike ründevektorite arv ja ründed muutuvad järjest keerulisemaks tänu interneti kättesaadavamaks muutumisele, selle kasutajate arvu suurenemisele, lisaks arendatakse välja uusi tehnoloogilisi lahendusi ning kasvab erinevate teenuste arv. (Majandus- ja Kommunikatsiooniministeerium, 2014)

Kuna igapäevaselt kasutatakse erinevaid termineid: infoturve (Riigi Infosüsteemi Amet, 2008), digitaalne ohutus (Lorenz, 2017) või interneti ohutus (Vetik, 2015), siis töö autor kasutab töös terminit küberkaitse, sest riik on selle nii sõnastanud.

> *"Infoturbe eesmärgiks on kaitsta informatsiooni, olgu siis tegemist paberil, arvutis või ka peas salvestatud informatsiooniga. See on turvameetmete loomise, valimise ja rakendamise protsesside kogum. IT-turve tegeleb esmajoones elektrooniliselt salvestatud informatsiooni ja selle töötlemise kaitsmisega."* (Riigi Infosüsteemi Amet, 2008, lk 24)

Riigi mõistes on küberkaitse see, kuidas riik korraldab oma info- ja sidesüsteemide kaitse, mis toetavad kriitilise infrastruktuuri toimimist, selleks on ajakohased turvameetmed nii infotehnoloogilistele lahendustele, organisatoorsetele kui ka füüsilistele nõuetele. (Kaitseministeerium, 2008) Petükis "Küberkaitse päevakorralisus ja igapäevane turvalisus" on välja toodud juhised ja soovitused riigiasutuste poolt, kuidas üksikisik saab panustada üldisele turvalisusele.

Antud töös käsitleb autor eelkõige kutsekoolide õpilaste küberkaitsealaste teadmiste laiendamise probleeme. Kutsekooli lähevad teiste seas õppima ka põhikooli lõpetajad, kes võivad olla väga naiivsed ja usaldavad, seeläbi on nad head sihtmärgid küberkurjategijatele. Peale kutsekooli lõpetamist sisenetakse kohe tööturule, kus nad muutuvad oluliseks lüliks turvalisuse tagamisel tööandja juures. Kuna organisatsiooni turvalisus sõltub siiski üksikkasutaja oskustest, teadmistest ja kasutamisharjumustest, siis on reaalne oht rünnaku

ohvriks langeda üsna suur. Uute õppeainete lisandumine kutseõppes toob kaasa vajaduse vastavate õppevahendite järele. On vaja selliseid õppevahendeid, mis toetaksid õppe- ja ainekava õpiväljundite saavutamist.

DigiTurvise (Lorenz, Laugasson, Püvi & Laanpere 2014) uuringu aruanne toob välja, et Eestis napib nii ettevõtetes kui ka haridus- ja teadusasutustes asjatundlikkust küberturvalisuse küsimustes. Väikesearvuline hea väljaõppe ja süvateadmistega spetsialistide ring (nt Kaitseliidu Küberkaitseüksus) on küll olemas, kuid see jääb alla nii praegusele kui ka edaspidisele nõudlusele. Küberkuritegevust saab ennetada tõstes üldist teadlikkust riskidest, see aitab ennetada ohtusid ja aitab ära tunda intsidente ning annab oskuse neile reageerida. Teadlikkust saab ja tuleb tõsta kõigi tasemete haridusasutustes, selleks tuleb teha teavitustööd ning käsitleda üldisi küberteemasid. Samas ei piisa üksnes teadlikkuse tõstmisest, vaid on oluline ka saavutada positiivsed muutused inimeste turvakäitumistes. (Lorenz, Laugasson, Püvi & Laanpere 2014)

DigiTurvise (Lorenz, Laugasson, Püvi & Laanpere 2014) uuringu aruandes jõuti järeldusele, et üldhariduskoolides on vaja:

- kaasajastada informaatikat jt digipädevusi puudutavaid ainekavasid iga 3 aasta järel;
- tuleb digiturbealaste teemade käsitlusi muuta selliselt, et need tagaksid õpilaste teadmiste viimist vastavale tasemele, mis on teatud klassis määratud;
- vähemalt 2 tundi nädalas tuleks igas klassis minimaalselt digipädevust õpetada. Näiteks informaatika, eraldi aine või mõne teise aine raames. (Lorenz, Laugasson, Püvi & Laanpere 2014)

Kutsehariduse kohalt tehti ettepanek koostada enesehindamise tasemetöö, mille abil saab hinnata õpilaste digipädevust, sh turbealast. Nõuda kõikidelt õpilastelt IT tasemetöö sooritamist, kes omandavad keskhariduse. IT õppes tuleb suuremat tähelepanu pöörata internetile ja selle turvalisusele. (Lorenz, Laugasson, Püvi & Laanpere 2014)

Kübervägivald ja küberjulgeolek on kiiresti saamas valitsuste, haridusasutuste ja õpetajate. (Mishna et al., 2012) Senini on sellele üldiselt vähe tähelepanu pööratud. Samuti rõhutakse õpetajate ettevalmistus- ja täiendõppeprogrammide vajadusele, et õpetajad saaksid tõhusamalt õpetada ja ennetada kübervägivalda. Haridustöötajate jaoks on oluline olla teadlik kübervägivallast ja küberkiusamisest (Kowalski & Limber 2007). See aitab tuvastada rikkumisi ja annab sobiva sõnavara aruteludeks. Samuti aitaks see igast juhtumist õigesti aru saada ja osata anda vajalikku toetust. (Hanewald, R. 2008)

“Eesti elukestva õppe strateegia 2020” toob välja, et õppetööd aitab köitvamaks muuta ja avardada elukestva õppe võimalusi digitaalsete õppevahendite kasutamine. (Haridus– ja Teadusministeerium, Eesti Koostöö Kogu & Eesti Haridusfoorum. 2014) Seepärast otsustas töö autor koostada oma õppevahend PowerPoint programmi abil, näitlikustamiseks kasutatakse internetist vabalt kättesaadavaid pilte ja videolõike.

Varasemalt on Eestis sarnasel teemal teinud lõputöö, mis haakub käesoleva tööga, Sulo Seim „Sissejuhatus küberkaitsesse- küberkaitse alase algõppe kontseptsioon Eesti Kaitseväes“ (2013) ning Allar Vallaots „Küberkaitsealane õppemoodul sideväelasest ajateenijatele“ (2013). Sulo Seim’i töö eesmärgiks oli välja selgitada küberkaitsealase algõppe kontseptsioon turvateadlikkuse tõstmiseks Eesti Kaitseväes. Töö tulemusena koostas autor küberkaitsealase algõppe läbiviimiseks Eesti Kaitseväes ainekava nimetusega „Sissejuhatus küberkaitsesse,” mis põhineb oma eriala ekspertide arvamusel, arvestades kaitseväe iseärasusi. Allar Vallaots koostas küberkaitsealase elektroonilise materjal kaitseväe sideeriala ajateenijatele. Tema loodud õppematerjal puudutab võimalikult suurt osa küberohtudest ja samas mitte minnes süvitsi probleemidesse.

Käesoleva bakalaureuse töö eesmärgiks on koostada väljaõppematerjal kutsekooli õpilastele lähtuvalt küberkaitsespetsialistide seisukohast, tõstmaks nende teadmisi arvuti igapäevase kasutamise ohtudest ning tutvustada abivahendeid isikliku info kaitsmiseks. Loodav õppematerjal võiksid olla abivahendiks kutsekooli õpetajatele või täiskasvanu täiendkoolituste läbiviijatele, kellele eesmärk on oma koolitatavaid harida ohtude suhtes, mis varitsevad arvuti igapäevase kasutamise juures ja teadmiste ning oskustega isikliku info kaitsmiseks.

Autor soovib enda uuringus leida vastuseid järgmistele uurimusküsimustele:

1. Millised küberkaitsealased teadmised ja oskused on vajalikud kutsekooliõpilastele küberkaisteekspertide arvamuste põhjal?

2. Milline peab olema õppevahendi ülesehitus ja sisu?

3. Kuidas hindavad küberkaitseeksperdid koolitusmaterjali sisu ja vajalikkust?

Bakalaureusetöö koosneb järgmistest osadest: sisukorrast, lühenditest ja töös kasutatavatest mõistetest, sissejuhatusest, teoreetilistest lähtekohtadest, metoodikast, analüüsist, ning kolmest lisast, milleks on intervjuuküsimustik, eksperthinnangu küsitlusleht ning elektrooniline küberkaitsealaste algteadmiste koolitusmaterjal.

Küberohud

Ülevaade

Tänapäeval veedavad enamik inimesi väga palju aega küberruumis kas siis seoses tööga või isiklikest vajadustest tulenevalt. Raske on määratleda ohte küberruumis, kuna ründed on etteaimamatud, raskesti defineeritavad ja on teadmatus motiivi suhtes, samuti on raske eristada riikliku, riigivälise, era- ja avaliku sektori piire ning tegutsejaid. Küberohtudega võitlemine nõuab järjest kõrgemat väljaõpet, arenguvõimelist õigusruumi, head organisatsioonidevahelist koostööd ja ressursse, sest ohud muutuvad globaalsemaks ja keerulistemaks. (Kaitseministeerium, 2008)

Majandus- ja Kommunikatsiooniministeerium toob välja, et Eesti riigi olulised küberjulgeoleku ohud tulenevad majanduse ja elanikkonna ulatuslikust ning kasvavast sõltuvusest IKT taristust ja e-teenustest". Küberjulgeoleku strateegia keskendub riigikaitse võime arendamisele, tõhustamisele, küberkuritegevuse vastu võitlemisele ja elutähtsate teenuste tagamisele. Toetamaks nende valdkondade arenguid, kujundatakse õiguslikku raamistikku, arendatakse rahvusvahelist koostööd ja tõstetakse küberjulgeolekut tagavate spetsialistide teadlikkust. (Majandus- ja Kommunikatsiooniministeerium, 2014) Kaitsepolitseiamet näeb, et kõige suuremad riskid infoturbes on seotud inimestega ja eelõige infosüsteeme ning tehnikat haldavate isikute käitumisega. (Kaitsepolitseiamet, 2016)

Küberohtude sihtmärgiks võib langeda nii riik, ettevõtjad kui üksikisikud ning põhjuseks on tavaliselt raha ja mõjuvõim. Küberruumis on võimalik professionaalsel kurjategijatel saada kriminaalset tulu, kuna vahelejäämise risk on madal. Samal põhjusel saavad kurjategijad edastada vajalikku infot Eesti suhtes vaenulikele riikidele. (Riigi Infosüsteemi Amet, 2016)

Arvutisüsteemi kahjustamiseks või soovimatute toimingute tegemiseks on loodud pahatahtlikke tarkvaru, mida nimetatakse ründevaraks (Viiruste ja muu ründevara…, 2017), kahjurprogramm või kahjurtarkvara (Riigi Infosüsteemi Amet 2008), pahavaraks või kurivaraks (Arvutikaitse, 2018). Pahavara kirjutavad inimesed, kes soovivad saada majanduslikku kasu, teevad seda uudishimust või soovist huligaanitseda. (Arvutikaitse, 2018) Viimastel aastakümnetel on arvutiviiruste levik tekitanud suuri rahalisi ja majanduslikke kaotusi. (Zhang, Li, Peng, & Huang, 2017)

Microsofti tugiteenused (Viiruste ja muu ründevara…, 2017) toovad välja ründevara järgmised näited:

- viirused
- ussviirused
- Trooja hobused
- nuhkvara
- petturlik turvatarkvara

Kuidas aru saada, et elektroonilises seadmes on pahavara? Nendeks tundemärkideks võib olla see, et seadme töö on häiritud ja ei tööta nii nagu tavaliselt, kas siis on aeglane või "jookseb" pidevalt kokku. Üheks tüütuimaks tundemärgiks on hüpikreklaamid, mis ilmuvad pidevalt ekraanile. Lisaks, kui on märgata, et kõvaketas teeb ebanormaalselt palju tööd ka siis, kui ükski programm ei tööta. (Kook, 2016)

Paljud küberohud võivad tekkida ka elektrooniliste seadmete kasutajate teadmatusest, oskamatusest, hajameelsusest või lihtsalt halvast juhusest. Näiteks *WiFi* võrgu pealtkuulamine on väga lihtne, kuna tegemist on raadiolainetega. Võrgus liikuvaid andmeid on lihtne lugeda ja kasutajal ei pruugi olla aimugi, et võrku jälgitakse. Sellepärast peab kasutaja hoolikalt jälgima, milliseid andmeid avalikus WiFi võrgus edastatakse. (Kirna, 2006) Hajameelsuse või halva juhusena võib välja tuua näiteks andmekandja (n mälupulk) kaotamise, mis võib sattuda kurjategija kätte. Teadmatuse näitena võib tuua ka jääkandmetele mitte tähelepanu pööramise seadme müümisel. Seadmed tuleks enne müüki põhjalikult puhastada.

Arvutiviirused.

"Arvutiviirus on sõltumatu alamprogramm, mis ennast taastootes teostab süsteemides, teistes programmides või nendega seotud keskkondades manipulatsioone, mis ei ole kasutaja poolt kontrollitavad" (Riigi Infosüsteemi Amet, 2008, lk 22). Arvutiviirused kas rikuvad, kustutavad arvutis olevaid andmeid või kogu kõvaketta sisu, samuti võidakse viiruse levitamiseks kasutada meiliprogrammi, mis on ka kõige sagedasem ja lihtsaim viis kiirsõnumite kõrval. Arvutiviirused võivad olla peidetud internetist allalaaditavates failides, näiteks võivad need olla peidetud ka erinevatesse programmidesse või piraattarkvarasse. Kui ei tea, kes sõnumi või meilimanuse elektronkirjaga saatis, ei tohi kunagi seda avada. Arvutiviirused võivad olla maskeeritud naljakateks piltideks, tervituskaartideks või heli- ja videofailideks. (Viiruste ja muu ründevara…, 2017) Mõned viirused on lihtsalt ärritavad - ulatudes väikestest arvutifailidest kuni uskumatult suures suuruses kirjeteni, mis asuvad arvuti kõvakettal ja vähendavad süsteemi jõudlust. (Hughes, 2008)

Ussviirused.

Ussviirus on programmkood ja mis tavaliselt levib kasutaja sekkumiseta. Ta levib meilisõnumite, võrkude või operatsioonisüsteemi turvaaukude kaudu automaatselt. Arvuti nakatub näiteks meilimanuse avamisel, ussviirus skannib arvutis faile ja otsib neist meiliaadresse, mida kasutab nakatatud meilisõnumite edasisaatmiseks. Ussviirused võivad kahjustada arvutisüsteeme enne, kui avastatakse viirus, või tekivad probleemid arvuti ja võrgu töös ning need muutuvad ebastabiilseks. (Viiruste ja muu ründevara…, 2017)

Troojalased.

Troojalane ehk „Trooja hobune“ on teistesse programmidesse peidetud ründevara. Trooja hobused levivad viiruste, usside ja allalaaditud tarkvara vahendusel ega levita ennast ise. Tavaliselt siseneb Trooja hobune arvutisse usaldusväärse prorammi (nt ekraanisäästja) kaudu ja paigaldades operatsioonisüsteemi koodi võimaldab küberkurjategijal nakatunud arvutile juurde pääseda. (Viiruste ja muu ründevara…, 2017) Mõiste "Trooja hobune" on pärit Vana-Kreekast, kus 1184 eKr toimunud Trooja sõja ajal tungisid kreeklased Trooja linna hiiglasliku seest tühja puust hobusega. Kreeklaste sõdurid varjusid hobuse sisse, mis jäeti lepituskingituseks troojalastele, kes viisid selle oma linna. Öösel väljusid hobuse sees varjul olnud kreeklased ja avasid linna väravad. Trooja hobuseks nimetatakse midagi, millega viiakse pahatekitaja kavalusega kuhugi sisse. (Allas et al., 2008)

Nuhkvara.

Nuhkvara on programm, mis kogub kasutaja arvutist informatsiooni ning saadab selle edasi infost huvitatud osapoolele. Nuhkvara ei ole ainult ebameeldiv, vaid on ka ohtlik, sest nuhkvara saab kasutada vahendina välja uurimaks konfidentsiaalset ja tundlikku informatsiooni nagu nt paroolid. (Riigi Infosüsteemi Amet, 2008) Nuhkvara saab arvutisse installida omaniku teadmata ja see võib muuta arvuti konfiguratsiooni, koguda isiklikku teavet, jälgida interneti kasutamist, koguda andmeid reklaamimiseks või suunata veebibrauseri veebisaidile, mida ei kavatsetud vaadata. (Viiruste ja muu ründevara…, 2017)

Eesmärgiks võib olla kasutaja jälgimine, info kogumine või soov häirida seadme tööd, nii et kasutaja ei oma kontrolli oma arvuti üle, asjakohaseim oht on identiteedivargus, kuid see ei pruugi olla veel kõige ohtlikum tegevus. (Hughes, 2008) Pahavara võib arvuti võtta

enda kontrolli alla selliselt, et kasutab seda teisteks pahatahtlikeks tegevusteks. Näiteks muudab arvuti n.ö zombiks, mis kuulub robotvõrku ja keda saab kasutada osana teenustõkestus rünneteks teiste IKT süsteemide vastu.

Petturlik turvatarkvara.

Petturlik turvatarkvara on tarkvara, mis soovib arvuti kasutajaid panna arvama, et arvuti on nakatunud viirusega ja pakkudes võimalust laadida alla või osta toote, mis viiruse eemaldab. Need tooted jätavad endast usaldusväärse mulje, kuna nende nimes on sageli sõna Antivirus, Shield, Security, Protection või Fixer. Peale alla laadimist ja käivitumist saab petturlik turvatarkvara takistada mitmesuguste rakenduste avamist või anda teate, et usaldusväärsed ja olulised Windowsi failid on nakatunud. (Viiruste ja muu ründevara…, 2017)

Reklaamvara.

Reklaamvara on tarkvara, mis laetakse kasutaja arvutisse, mis esitab või kuvab automaatselt reklaame. Reklaamimaterjali kuvatakse pärast kasutaja arvutisse tarkvara installimist või teatavate arvutirakenduste ja veebilehtede avamise ajal. Sellepärast võib kasutaja leida oma arvutis ilmuvaid hüpikreklaame, mille teema on täpselt häälestatud kasutaja viimaste weebiotsingute teemade põhjal ja sagenevad, kui uurite samu teemasid. (Hughes, 2008)

Juurkomplekt ehk rootkit.

Termin rootkit viitab programmile, millel on arvutis juurõigused ja millel on kaasas tööriistad, millega arvutit manipuleerida. Juurõigused tähendab, et programmil on juurdepääs administraatori kontole süsteemis ja see annab programmile võimaluse failide muutmiseks. See on sarnane Windowsi operatsioonisüsteemi administraatoriõigusega. Rootkittidega seotud negatiivne konnotatsioon ei ole rootkit ise, vaid küberrünnakud, mis kasutavad rootkite oma eesmärgi saavutamiseks. (Luckett, McDonald, & Dawson, 2016)

Esimene eesmärk on luua ühendus, kasutades kaugpääsu liidest ja saavutada kontroll ning teine eesmärk on pealtkuulamine. Kui ründaja on saanud ligipääsu arvuti kaugpääsu liidesele, on tal võimalik protsesse käivitada ja süsteemifaile kontrollida. Kui eesmärk on

pealtkuulamine, installib ründaja nakatunud arvutisse nuhkvara. Rootkit, mis sialdab nuhkvara, võimaldab lugeda e-kirju ja salvestada klahvivajutusi, mida ründaja saab kasutada tundliku teabe hankimisel. Mõlemal juhul on ründaja huvitatud pikaajalisest juurdepääsust süsteemile. Rootkiti peetakse ründe järgseks vahendiks, sest see on sisse viidud rünnakutsükli lõpus ja kindlustab kurjategija kontrolli süsteemi üle. (Luckett, McDonald, & Dawson, 2016)

Social Engineering e andmepüük e sotsiaaltehnoloogia.

Püüdlust inimesi võrgus psühholoogiliselt mõjutada, nendega manipuleerida ja emotsionaalselt rünnata ebaseaduslikku kasu saamise eesmärgil nimetatakse ”social engineering”. (Atkins & Huang, 2013) Üldiselt keskendutakse üksikisikute manipuleerimisele ja julgustamisele ohtlike toimingute tegemiseks, nagu näiteks pahavara sisaldava e-posti manuse avamine või inimeste veenmine konfidentsiaalse teabe avaldamiseks nagu näiteks kasutajate kontod või paroolid (Mitnick & Simon, 2006). Näiteks näevad andmepüügiga seotud e-kirjad välja nagu usaldusväärse organisatsiooni või asutuse poolt loodud (Greitzer et al., 2014) ning järjest enam kasutatakse asutuste logosid ja veebisaitide aadresse ja viiteid, mis tunduvad olevat legitiimsed (Workman, 2008).

Williams, Beardmore, & Joinson (2017) uurivad oma artiklis seda, miks on internetipettused nii tõhusad ja mis teeb inimesi neile eriti vastuvõtlikuks. Internetipetturid loovad stsenaariume, milles sihtmärk reageerib piisavalt kindlalt, kasutades sageli paanikat, põnevust, uudishimu või empaatiat puudutavaid emotsionaalseid käivitavaid tegureid, et julgustada inimesi vigu tegema oma otsuste langetamisel. (Langenderfer & Shimp, 2001). Sellised stsenaariumid sisaldatavad tavaliselt loteriivõitu, psühholoogiliselt ettevalmistavat sisu, veebipõhiste kontode peatamist või internetipõhist romantikat. (Williams, Beardmore, & Joinson, 2017).

Inimesed lasevad ennast mõjutada. Kui inimesed näevad potentsiaalset ohtu ja neile pakutakse meetmeid, kuidas ohule reageerida, siis nad tõenäoliselt ka kasutavad neid meetmeid, et vältida kahju isiklikule varale. (Ruiter et al., 2014) Inimesed, kes üritavad teisi mõjutada, kasutavad selliste lähenemisviiside eeliseid, luues stsenaariumi, mida tõlgendatakse kui ohtu (näiteks konto turvalisusrikkumist) ja selle ohu vähendamiseks lihtsat toimingut (nt konto üksikasjade kontrollimiseks lingi klõpsamine). (Williams, Beardmore, & Joinson, 2017) Näiteks pangaandmete uuendamise päring meilitsi, mis deklareerib, et on oht, et kasutaja andmed lekkisid ja neid tuleks uuenda ning lisatud on link panga kodulehele.

Tarkvara turvaaugud.

Infotehnoloogia tooted kannatavad mitmesuguste turvanõrkuste all tarkvara vigade tõttu. Need vead võimaldavad kasutada haavatavusi süsteemi turvalisuse kompromiteerimise eesmärgil. Kui vastav kasutaja avastab haavatavuse, suureneb sissetungide risk, kuni tarkvara tootja laseb välja vastava turvaplaastri. Turvaplaastri paigaldusprotsess aitab säilitada tarkvara stabiilsust ja vähendab kahju tõenäosust. Pärast turvaplaastri levitamist ja paigaldamist on haavatavus eemaldatud. Haavatavuste paikamise või süsteemi uuenduste ärajätmine loob rohkem nõrku kohti ja põhjustab katastroofilisi tagajärgi organisatsioonidele ja kasutajatele. Seetõttu on turvaplaastri edukas implementeerimine ka vältimatu tegur, mille alusel saab sissetungimise määra hinnata. (Kansal, Kumar &, Kapur 2016)

Küberkuritegevus.

Küberruumis tegutseb väga erineva tasemega küberkurjategijaid, alustades petukirjade levitajatest kuni oskuslike ja oma ründeid hoolikalt planeerivate infosüsteemikaaperdajateni välja. Riigi Infosüsteemide Ameti küberturvalisuse teenistuse 2016. aasta kokkuvõttes on näha, kuidas küberkurjategijate oskused arenevad pidevalt, kohanedes nii tehnoloogiliste muutuste kui turuolukorraga. Levima on hakanud küberkuritegevuses ka „teenuse" pakkumine neile, kellel endal pole vajalikke oskusi ja teadmisi. (Riigi Infosüsteemi Amet, 2016)

Küberkuritegevuses ei ole geograafilisi piiranguid, iga digiseadme kasutaja on potentsiaalne sihtmärk, saamaks temalt raha või rahalist väärtust omavat teavet. Halvimal juhul kasutatakse tema seadet hüppelauana teiste isikute või ühenduste ründamiseks. Küberründe kaudu välja petetud teavet (näiteks krediitkaardiandmed, kasutajanimed ja paroolid) müüakse kuritegelikele ühendustele edasi või kasutatakse arvutikelmuste toimepanemiseks. Kuritegelikku tulu teenitakse ka väljapressimise abil, kus arvuti pahavaraga nakatatud arvutit kasutatakse teenusetõkestusrünneteks. Krüptolunavara, teenusetõkestusründeid ja andmevargust kasutatakse selleks, et nõuda ohvrilt raha või virtuaalraha Bitcoini. Vastutasuks lubatakse rünne lõpetada või andmeid hoida ja neid mitte avaldada. 2016. aastal toimus selline väljapressimine ka Eestis, kus põhiseaduslik institutsioon sai sellesisulise kirja, kus ähvardati teenusetõkestusrünnetega, kui ei tasuta nõutut summat. (Riigi Infosüsteemi Amet, 2016)

Lunavara.

"Lunavara (ransomware), tuntud ka kui krüptoviirus või krüptouss, on selline pahavara, mis krüptib kasutaja arvutis kas teatud olulised andmed või terve kõvaketta, misjärel kurikaelad nõuavad andmete lahtikrüptimisvõtme eest lunaraha. Viimase maksmine, muide, ei garanteeri veel seda, et ohver ka krüptovõtme kätte saab." Arvutisse satub lunavara tavaliselt muu pahavaraga, näiteks spämmi, hooletult arvutisse ühendatud andmekandja või pahatahtliku kodulehe külastamise kaudu. Seda saab ära hoida toimiv viirustõrje ja värske varukoopia tegemine. (Arvutikaitse, 2018)

Küberkiusamine.

Küberkiusamine on tegevus, kus keegi kiusab kedagi, saates alandava, hirmutava ja ähvardav sisuga teateid, kasutades sotsiaalmeediat või teisi interneti kanaleid nagu e-kiri, jututoad ja tekstsõnumid. Küberkiusamine seisneb tavaliselt ohvri ähvardamisega või šantažeerimisega. Tavaliselt kasutatakse selleks ohvriga seotud alandavaid kirju, fotosid või videoid ning ähvardatakse nende avalikustamisega sotsiaalmeedias või muus avalikus veebikeskkonnas. Võidakse kasutada ka võlts veebikontosid ja variidentiteeti foorumite jms kommenteerimisel. Küberkiusamise tuvastamine on tihti keeruline, kuna ohvritel on hirm häbistava materjali avalikustamise ees ning nad ei esita süüdistust. (Politsei- ja Piirivalveamet, 2018)

Politsei- ja Piirivalveamet annab soovitusi, kuidas tõkestada küberkiusamist:

1. Kui keegi saadab mõnes virtuaalses suhtluskanalis mõnitava ja halvustava sisuga sõnumeid ning teateid, siis blokeeri suhtluskanalites kiusaja teda eelnevalt sellest teavitades.

2. Kopeeri halvustava sisuga teated, et neid saaks kasutada tõenditena.

3. Suhtlusportaalides teavita portaali pidajat kiusaja tegevusest. (Politsei ja Piirivalveamet, 2018)

Küberkaitse päevakorralisus ja igapäevane turvalisus

Antud töös lähtub autor rohkem riigiametite poolt antud või riigiasutuste poolt tellitud uuringute suunistest ja juhenditest, kuidas tõsta teadlikkust, hinnata ohte ja käitumisjuhistest.

Teadlikkuse tõstmise juures on oluline arusaada, et iga arvuti, arvutivõrgu või infosüsteemi omanik vastutab tema valduses oleva IT- ja IKT vahendite sihtotstarbel ja heaperemeheliku kasutamise eest, see tagab küberruumi turvalisuse. (Majandus- ja Kommunikatsiooniministeerium, 2008)

Riigi Infosüsteemi Ameti andis hinnangud ja ennustused 2017. aastaks: (Riigi Infosüsteemi Amet, 2016, lk 49-50)

- *Elutähtsate teenuste kübersõltuvus kasvab.*
- *Avalik sektor on nii juhuslike kui suunatud rünnete sihtmärk.*
- *Erasektori teadlikkus küberriskidest on lünklik nii üksikisiku kui ettevõtjate tasandil.*
- *Küberkuritegevus on üha professionaalsem.*
- *Eesti on jätkuvalt Venemaa mõjutustegevuse sihtmärk.*
- *Arenevad tehnoloogiad ja teenused on haavatavad ning turvalisus ei jõua tehnoloogia arenguga sammu pidada.*
- *Enamiku registreeritud küberintsidentide põhjus või seda soodustav tegur on aegunud tarkvara.*
- *Üksnes salasõnadel põhinev autentimine ei ole enam turvaline.*
- *Õiguskeskkond vajab ajakohastamist.*

2016. aastal suunas Riigi Infosüsteemi Ameti oma tähelepanu ennekõike lõppkasutajate teadlikkuse tõstmisele. Kodulehe ja sotsiaalmeedia kanalite kaudu anti praktilisi tegevusjuhiseid krüptolunavara vältimiseks, e-posti kontode kaitsmiseks ja sotsiaalmeedias varitsevate ohtude eest hoidumiseks. Kasutusele võeti tugevam krüptograafia riiklikes isikutuvastusvahendites ja seepärast juhendati, kuidas ID-kaartide, elamisloakaartide ja digi-ID dokumentide krüptograafilist sisu kauguuendamise teel asendada. (Riigi Infosüsteemi Amet, 2016)

DigiTurvis (Lorenz, Laugasson, Püvi & Laanpere 2014) toob välja kasutajate olulised põhimõtted digivahendite igapäevase turvalise kasutamise kohta:

1. *turvaline veebilehitsemine*
   - *privaatse režiimi käivitamine ja selle vaikimisi määramine;*
   - *kogemata veebilehitsejale meeldejäetud kasutajate, salasõnade kustutamine;*
   - *krüpteeritud veebipõhine identiteedihaldamine (nt lastpass.com vms);*
   - *võimalusel turvalise ühenduse (https) kasutamine;*
   - *veebilehe identiteedi jälgimine (vt Google soovitused2);*
   - *turvaliste lisandite kasutamine veebilehitsejates (nt Adblock Plus3, Ghostery4);*
   - *teadlikkus erinevatest veebilehitsejatest läbi turvalisuse vaatepunkti*
2. *igapäevane arvutikasutamine ei peaks toimuma administraatori õigustes*
3. *piisava turvalisusega salasõna valimine, selle turvalisuses veendumise võimaluste tutvustamine (nt)*
4. *arusaamine, milliseid programme, käske, väliseid seadmeid võib usalda ja käivitada, arvutiga ühendada*

5. *pahavara tõrjumisvahendid (tulemüür, viirusetõrje, nuhkimisprogrammide eemaldaja, veebilehitseja turvamine)*
6. *nutiseadmete turvamine, sh traadita andmeside turvamine (sh WiFi krüpto, VPN kasutamine – eriti avalike ühenduste puhul)*
7. *millal on mõistlik oma arvuti või nutiseade võrku ühendada ja millal mitte*
8. *e-posti kasutamine: miks ja kuidas saata kirja mitmele inimesele pimekoopiana*
9. *kasutatava tarkvara perioodiline uuendamine, tutvustada ka kogu rakendustarkvara koos operatsioonisüsteemiga kiire uuendamise võimalusi*
10. *teadlikkus erinevatest operatsioonisüsteemidest ja nende turvalisusest – tutvustada tarkvara digitaalset allkirjastamist pakkuvaid operatsioonisüsteeme*
11. *virtualiseerimise võimalused, sh turvalisuse vaatepunktist lähtuvalt*
12. *pilvepõhiste salvestusvõimaluste valik, sh turvalisuse vaatepunktist*
13. *failide varundamise tähtsusest ning turvalisusest ja ristkasutuse võimalustest eri seadmete ja kasutajate vahel*
14. *kuidas avastada ja tulla toime pahavaraga ning seda tulevikus vältida*
15. *kuidas avastada ja tulla toime küberründega ning seda tulevikus vältida*
16. *kuidas hallata digitaalset jalajälge ehk siis infot enda kohta internetis – millal ja millist infot endast veebi panna ning kuidas sellele ligipääsetavust hallata*
17. *miks on vaja ja kuidas hoida füüsilist tervist ja kuidas nutivahendid ja ka tarkvara arvutis, internetis seda teha võivad aidata – võimalus ka õpilastevaheliseks võistlemiseks*
18. *teadlikkus nuhkimise, jälitamise võimalikkusest ja kuidas seda vältida ning mida teha, kui on juhtunud intsident*
19. *teadlikkus sotsiaalse manipuleerimise eri tahkudest ja kuidas neid vältida ning mida teha, kui on juhtunud intsident* (lk 21-22)

DigiTurvis (Lorenz, Laugasson, Püvi & Laanpere 2014) annab tavakasutajale soovitusteks:

1. *Ära ava manuseid ja linke, mille usaldusväärsuses sa kindel ei ole.*(...) *Kahtlane e-kiri edasta koos päiste ja manusega aadressile cert@cert.ee (või laadi üles https://paste.cert.ee) ning kustuta kiri ise kohe.* (lk 10)
2. *Ära maksa lunaraha, see toetab vaid kuritegevust ega garanteeri failide tagasisaamist. Kui lahendust failide taastamiseks veel ei ole, hoia nakatunud kõvaketas siiski alles: üldjuhul taastamisvõimalus varem või hiljem tekib.* (lk 10)
3. *Parim kaitse lunavara vastu on tagavarakoopia ja seejuures on andmete regulaarne varundamine väga oluline. Kui sa ise ei oska oma arvutist või nutiseadmest tagavarakoopiat teha, pöördu asutuse IT-toe või tuttava IT-spetsialisti poole.* (lk 10)
4. *Enne parooli ja kasutajanime sisestamist veendu, et tegemist on tegeliku teenusepakkuja veebilehega. Kui aadressiribal kuvatav veebiaadress tekitab kahtlusi, ei tohi sinna oma andmeid sisestada ja kui oled oma parooli juba sisestanud, vaheta parool kohe.* (lk 13)
5. *Ära saada raha ega vasta petukirjale. Kui raha küsiva kirja on saatnud sõber, helista talle ja uuri järele, kas ta on tõesti hädas. Kui oled petukirja saatjale juba raha saatnud, pöördu kindlasti politseisse (cybercrime@politsei.ee) ning hoia uurimise tarbeks alles küberkurjategijatega peetud kirjavahetus.* (lk 13)
6. *Lülita võimalusel sisse kaheastmeline autentimine, eriti e-posti kontol. Juhendid selleks leiad RIA blogist (blog. ria.ee).* (lk 13)
7. *Kahtlasest aadressist või õngitsuskirjast anna teada e-posti aadressil cert@ cert.ee.* (lk 13)

8. *Väldi oma tööaadressi sidumist pilveteenuste või eraviisiliseks kasutamiseks mõeldud kontodega. Selline tegevus lihtsustab tuntavalt küberkurjategijate ja vaenulike võõrriikide luureteenistuste sihitud rünnakuid ametialaste kontode vastu, sest tekib võimalus leida miljonite kasutajate hulgast just need kasutajad, kelle paroolide murdmisele ja andmete kättesaamisele tasub aega ja vaeva kulutada.* (lk 21)
9. *Väldi paroolide ristkasutamist, eriti tööarvuti parooli kasutamist teistes teenustes. Kus vähegi võimalik, lülita sisse kaheastmeline autentimine.* (lk 21)

Politsei- ja Piirivalveamet (2018) annab turvalise parooli kohta soovitusteks:

1. Alati kasuta turvalist ja unikaalset parooli.

2. Parooli pikkus peab olema vähemat kaheksa tähemärki.

3. Parool peab olema unikaalne ja ei tohi ristkasutada erinevate kontode või seadmete vahel.

4. Parool peab sisaldama suuri ja väikeseid tähti, numbreid ja kirjavahemärke.

5. Vältida tuleb reaalseid või sagedasti kasutatavaid sõnu. Näidetena tuuakse K3.o))s7 või Sa1.baNaan82

6. Ei tohi olla omanikuga seostatav (nimi, mõni kuupäev jne)

7. Paroole ei tohi teistega jagada.

8. Parooli sisestades jälgi, et keegi ei loeks mida sisestad ja ära unusta ennast avalikest seadmetest välja logida.

Turvaliseks parooliks annab Sibold (2016) soovitusteks:

1. Ühte ja sama parooli ei tohi erinevates kohtades kasutada, sest muidu saavad kurjategijad kõigi sinu kontodele ligi.

2. Selleks, et kurjategijad ei saaks ohvri parooli ära arvata, tuleks kasutada keerulisi ja pikkasid ehk tugevaid paroole.

3. Tugev parool peaks sisaldama sümboleid, tähti ja numbreid.

4. Vaheta paroole regulaarselt.

Õppevahend

Õppevahenditega töötavad õpilased kuni 90% õppeajast (Mikk 1999), seega peab õpetajatel olema häid õppematerjale, mida nad saavad kasutada parema õpitulemuse saavutamiseks. (Sleuers, 2001). Oluline on, et õppematerjali maht vastaks õpilaste võimetele seda omandada, väga mahukad õppevahendid ei arenda mõtlemist. (Mikk, 2001) Samuti tuleb jälgida, et tekst ei oleks liiga keerukas või lihtne, mis ei anna uusi teadmisi, ei arenda mõtlemist ja on igav. (Mikk, 2000) Probleemiks on ka lähenemine, et ühesugune materjal sobib kõigile, arvestamata õppija eelnevaid teadmisi ja oskuseid. Seeläbi võivad õppijad olla koolitusest pettunud, kuna nad ei õppinud midagi juurde. (Valentine, 2006; Schultz, 2004) Koolituste sisu ja ulatus sõltub koolitatavate eelteadmistest ja sihtrühmast. Üldine turvalisuse haridus on tavaliselt suunatud kolmele tasemele: üldine julgeolekualane teadlikkus, treening või haridus. (Reid, Niekerk & Solms, 2011)

Teadlikkuse tase koosneb teadlikkust tõstvatest tegevustest, mille eesmärk on inimesi antud teema osas kaasa tõmmata ehk äratada huvi. Sihtrühm on laiem üldsus, kes on passiivsed info vastuvõtjad ning õpitud teadmised on neil tavaliselt lühiajalised, vahetud ja konkreetsed, juhul kui õpitut ei korrata korduvalt. See tase vastab küsimusele "mis". Sellist taset saab õpetada plakatite, flaierite, videode ja kaubamärkide reklaamplakatite ja – loosungitega. (Katsikas, 2000)

Teine tase vastab küsimusele „kuidas” ja see tähendab süvendatud õpet, mis annab oskuse probleeme lahendada. Õpe põhineb olemasolevatel meetoditel ja lahenditel, mis tähendab, et kuigi õpingud kestavad kauem ja omandatakse konkreetsed oskused, vananevad need teadmised kiiresti. Sellises olukorras tuleks täpsemalt hinnata õpetatava baastaset, koolitusvajadusi ja koolituse eesmärki. Kõigile ei olegi vaja ühesugust teise taseme väljaõpet. Antud olukorras tuleks rakendada erineva raskusastmega õpet s.t algajast kuni edasijõudnuni. Koolitusformaatide näideteks on loengud, interaktiivsed demostratsioonid, juhtumiuuringud ja iseseisev harjutamine. (Katsikas, 2000)

Kolmas tase ehk erialane haridussüsteem keskendub eksperttasemele, kus õpetatav läbi oma kogemuste ja teadmiste omandab tervikliku arusaama kogu valdkonna kohta. Vähem tehnilist ekspertide koolitusformaati saab kasutada ka tavainimeste koolitamiseks. Oluliseks õppe-eesmärgiks siis on luua teadmised ja oskused tasemel, mis vastab küsimusele „miks“.

Selline tase saavutatakse näiteks osalemisel seminarides, aruteludes, uurimustes või ise lugedes. (Katsikas, 2000)

Küberjulgeolekus on olulisem tõsta teadlikkuse taset ja seda taset saab tõsta haridus- ja koolitusprogrammidega. Oluline on, et kasinate küberturvalisuse teadmistega inimesed saavad aru seosetest, rollist ja vastutusest. Kuid neid programme koostavad tihti turvaspetsialistid, kes ei oma pedagoogilist haridust ning sellest tulenevalt ei pruugi olla pädevad antud teemade sellisel käsitlemisel ning õppematerjalide koostamisel. (Reid, Niekerk & Solms, 2011)

Õppijat motiveerivad materjali omandama sobiva raskusastmega tekstid ja selge eesmärk. (Krull, 2000) Õppija omandab materjali paremini, kui ta seda väärtustab ja peab oluliseks (Krull, 2000) ja mis ei ole liiga raske ega elukauge (Mikk, 1993; Peterson, 2003). Teksti keerukusest sõltub, kui jõukohane on see õppijale, selle sisu peab olema huvitav ja vanusele kohane. Tekst ja laused ei tohi olla liiga pikad. Õppija taustteadmisi arvesse võttes peab autorteadlikult arvestama mõistetava teksti ja lihtsa keele reegleid. (Mikk, 1993; Peterson, 2003)

1985. aastal viidi edukalt läbi programm Austraalias Lavertoni koolis, kus rakendati mõtlemise arendamiseks mõtlemisküsimusi. Mõtlemisküsimusteks nimetati neid küsimusi, millele õpikus otsest vastust ei olnud. Mõtlemisküsimused algavad sageli sõnadega "miks", "kuidas", "mis oleks, kui" jne ning võimaldavad pikemaid vastuseid. (Mikk, 1993) Läbitöötatud materjali kohta küsimuste esitamine toetab teadmiste omandamist, arendab arutlusoskust ja aktiveerib mõtlemist. (Krull, 2000)

Küsimuste olulisuse toob välja ka Katsikas (2000), mis tasemel peab asutuse juhte infosüsteemide turvalisuse riskidega seoses harima. Kas tuleb tõsta nende teadlikust nii, et nad oskaksid vastata küsimusele üldiselt, et mis on infoturve s.t hoides nende teadmisi üldisel tasemel selliselt, et nad tunneksid ära teema ja sellega seonduva. Või tuleb harida neid nii, et nad suudaksid teemat käsitleda ja vastata küsimusele, kuidas turvalisust tagatakse? Või tuleb tõsta nende teadmisi kognitiivsel tasemel ja nende õppimiseesmärke oskuste tasemel? Või tõsta üldse nende teadmiste teadlikku taset ja viia nende õpieesmärgid mõistmise tasemele, et nad suudaksid anda põhjaliku ülevaate infoturbe küsimustes oma asutuse kohta.

Giannakas, Kambourakis, Papasalouros ja Gritzalis (2016) toovad oma töös välja, et küberjulgeolekualast õppematerjali omandatakse paremini, kui õppetöös osalevad motiveeritud õpilased ja kasutatakse uudseid õpivahendeid. Seega peab õppevahend olema koostatud nii, et see suurendaks õppijate motivatsiooni materjali omandada. Näiteks

nutivahendi mäng CyberAware on probleemide lahendamise keskkond, kus õpilane täidab mitmeid erinevaid ülesandeid ja väljakutseid. Kuna tehnika ja sellega seonduv areneb tormilise kiirusega, siis on oluline ka õppematerjali ajakohasus. (Giannakas, Kambourakis, Papasalouros & Gritzalis, 2016; Reid, Niekerk ja Solms, 2011)

Reid, Niekerk ja Solms (2011) toovad välja probleemi, et enamikul tänapäevastel infoturbeharidusepoolsetel lähenemisviisidel ei ole usaldusväärset teoreetilist alust ning see võib viia nende haridusprogrammide ebaõnnestumiseni. Sellised küberjulgeoleku haridusprogrammid peaksid tuginema kindlatele pedagoogilistele teooriatele.

Suureks probleemiks on see, et inimesed ei ole motiveeritud ennast infoturbe alal harima. Valentine (2006) selgitab, et need töötajad, kes ei tegele organisatsiooni tundliku informatsiooniga, ei hooli infoturbest ega oma ka teadmisi võtetest, kuidas inimestega manipuleeritakse. Samuti on probleemiks see, et inimesed kipuvad unustama, mida nad erinevatel koolitustel õppisid, ning seetõttu on need koolitused kasutud, kuna inimesed pole midagi tõepoolest õppinud. (Reid, Niekerk & Solms 2011) Üheks unustamise põhjuseks võib olla see, et koolitusmaterjali koostavad julgeolekutöötajad, kellel pole alati pedagoogilist kogemust ja sellisel juhul võib materjali omandamine olla raskendatud. Lisaks koolitavad mitte IT erialast personali mitte IT erialased inimesed, mis on ka üheks põhjuseks, miks inimesed ei omanda õpetatud materjali. Vastupidi, pedagoogide poolt pakutavad õppematerjalid ei pruugi olla piisavalt põhjalikud ega anna edasi terviklikke erialaseid teadmisi. (Reid, Niekerk & Solms 2011) Schultz (2004) tõi välja, et inimestele võiks õpetada erialaseid teadmisi, mis nende igapäevaelus kasulikud ja rakendatavad on. (Reid, Niekerk & Solms 2011)

Küberjulgeoleku haridusprogrammide üks pedagoogiliselt usaldusväärne lähenemisviis võiks olla “aju ühilduv õppimine”. (Reid, Niekerk & Solms, 2011) Sellise õpetuse viisi eesmärk on sobituda aju füsioloogilise arenguga, selle asemel, et sundida aju kohanduma etteantud korraldustele arvestamata aju füsioloogilisi omadusi õppimise seisukohast. Aju ühilduva õppe meetodite loomisel on arvesse võetud, et õppimise protsess tekitaks inimese ajus füsioloogilisi muudatusi, mille eesmärk on luua närvi rakkude püsivaid sünapse ehk ühendusi, läbi mille õpitud paremini meelde jääb. Meetodid on kohandatud aju arengu füsioloogiat silmas pidades. (Caine & Caine, 1991; McGeehan 2001)

Aju ühilduva õppe üks olulisemaid põhimõtteid on "Õppimine läbi emotsiooni". (Caine & Caine, 1991; McGeehan 2001) Kõik, mida õppijad õpivad, on emotsioonide ja

mõttelaadi poolt mõjutatud ja korraldatud. Emotsioonide ja mõttelaadi, mis sisaldab ootuseid, erapooletust, eelarvamust, enesehinnangut ning suhtlusvajadust. (Caine & Caine, 1991). Õppuri meelelaad ja emotsionaalne seisund mõjutavad tema keskendusmisvõimet, seega avaldatakse mõju ka tema õppimise võimele. Reid, Niekerk ja Solms (2011) näevad, et tunnetusliku ja emotsionaalset poolt ei saa lahus hoida. Selle põhimõtte rakendamine seoses küberjulgeolekualase haridusega eeldab, et kursuse sisu tuleks esitada selliselt, et kursuse sisu toetaks seda meetodit, mis ei tekita hirme ja soodustab ühist lähenemist õppimisele.

Teine aju ühilduv põhimõte on see, et aju talletab kõige efektiivsemalt infot, mis on õppija seisukohast oluline (Caine & Caine, 1991; McGeehan 2001). Caine ja Caine (1991) selgitavad seda kui "mustri tekitamist". Õppimisprotsessi ajal püüab aju eristada ja mõista mustreid, mis esile tulevad ja mida õpiti või kogeti. Seega tuleb materjali esitada viisil, mis soodustab probleemide lahendamist ja kriitilist mõtlemist (Reid, Niekerk ja Solms 2011).

Reid, Niekerk ja Solms (2011) töötasid välja küberkaitse alase koolituse ülesehituse üheksa peatükki:

1. Turvalisus üldiselt - sissejuhatav selgitus turvalisuse ja turvalisus ega seotud terminoloogia

2. Infoturve - selgitus julgeolekualase teabe olulisusest ja selle teabe turvalisuse tagamise meetoditest;

3. Parooli turvalisus – teadmised, kuidas valida turvalist parooli;

4. Viirusteadlikkus - teadmised erinevatest viirustest, nende avastamise ja ennetamise kohta;

5. Andmesalvestus ja varundamine – teadmised, kuidas säilitada andmeid turvaliselt;

6. Arvutieetika - arvutikasutaja asjakohane käitumine;

7. Töökoha distsipliin - näitab, kuidas süsteemi kasutajad peaksid töökeskkonnas käituma;

8. Riistvara turvalisus - käsitleb riistvaraseadmete kaitset;

9. Sotsiaaltehnoloogia ehk *Social Engineering* - hõlmab sotsiaaltehnoloogiat ja selle rünnakute vastu võitlemise meetodeid.

CyberAware rakendusega seotud õpieesmärke võib kokku võtta järgmiselt:

1. Õpilased peavad suutma tuvastada küberjulgeoleku tehnoloogiad, mida interneti-ühendatud seade peab sisaldama, selleks et kasutaja saaks küberruumis turvalisust hoida.

2. Õpilased peaksid suutma väärtustada ja hinnata igat küberjulgeoleku tehnoloogiat ja selle pakutava kaitse taset.

3. Võttes arvesse reaalseid internetikasutusvõimalusi, peaksid õpilased olema võimelised tuvastama ja valima rünnakute tõkestamiseks õige kaitsetehnoloogia. (Giannakas, Kambourakis, Papasalouros & Gritzalis, 2016)

Metoodika

Meetodite valik

Käesolevas bakalaureusetöös kasutab autor küberkaitseeksperide arvamuste uurimisel kvalitatiivset induktiivset sisuanalüüsi. Analüüsis on tegemist suuremahuliste tekstide temaatilise eristamise ja kategoriseerimisega. Temaatilise sisuanalüüsi puhul kasutatakse kodeerimist ja nendest koodidest luuakse kategooriad. (Stemler: 2001) See võimaldab eristada olulisemaid ja vähem olulisemaid kategooriaid, siis lihtsustub tekstide analüüs ning saab keskenduda eeskätt uurimuse olulisematele teemadele sõltuvalt uurimuse eesmärkidest. (Stemler: 2001) Temaatiline sisuanalüüs toob nähtavale varjatud tähendusi (Ezzy 2002: 88-89), uurimuses osalejate arvamusi ja hinnanguid (Õunapuu, 2014).

Töös kasutati andme kogumiseks temaatilist poolstruktureeritud intervjuud (Lisa 1), jättes intervjuu käigus võimaluse lisaküsimusteks ja aruteluks. (Laherand, 2008) Intervjuu küsimustik koostamiseks kasutati antud töö teoreetilisest osast. Autor soovis uurida, missugused on küberkaitseekspertide soovitused õppematerjali koostamisel kutsekooliõpilastele. Antud teema vajab paindlikku lähenemist, kuna küberkaitseeksperte on vähe ja nende tase ja kogemused on erinevad. Intervjuud lindistati digitaalselt kahe seadme poolt ning hiljem transkribeeriti. Jälgiti transkribeerimisnõudeid (Laherannale, 2008) ja rääkija kõne pandi kirja võimalikult täpselt. Intervjuu salvestamiseks kasutati programme Microsoft Corporation Kõnesalvesti ja Voice Recorder, nendega kuulati hiljem salvestusi. Intervjuude analüüs toimus kolmes etapis: 1. intervjuu transkribeerimisest *Microsoft Wordi* programmi abil, 2. kodeerimisest, kus sõnadele ja fraasidele anti koodid ja 3. koodid kategoriseeriti.

Väljavõte E3 intervjuu analüüsist:

"…See on siis antiviirused, tulemüürid, pop upide blockerid (…) Lisaks siis, et arvutid oleksid uuendatud, et neil oleksid peal viimased värskemad uuendused jne …"

Põhikategooria	**Alamkategooria**	**Koodid**
Küberkaitse meetmed	Ohud	Pahavara
		Õngitsus- ja petukirjad
		Võltsveebilehed
		Sotsiaalmeedia
		Identiteedi vargus
		Andmete leke
		Kelmused

		Küberkiusamine
		Sõltuvused (Online kasiino, kihlveod, mängud, sotsiaalmeedia jne)
		Tervisehäired (füüsilised ja vaimsed)

Tabel 1. Kategooriate moodustamise näide

Küberkaistealaste algteadmiste õppematerjali koostamisel on lähtutud antud töö teooriaosast ja empiirilisest uuringust. Õppematerjali loomiseks kasutati *Microsoft Powerpointi* programmi. Õppematerjal on loodud uuringust ja teooriast saadud sisendi alusel. Koostamisel kasutati "aju ühilduv õppimine" põhimõtteid, näidates koolitatavatele, et nad puutuvad küberohtudega igapäevaselt kokku ja antud valdkond on neile isiklikult tähtis.

Lisaks videotega püütakse tekitada emotsiooni, sest kõik mida koolitatavad õpivad, on mõjutatud emotsioonide ja mõttelaadi poolt. Õppematerjali kasutamise metoodika on loeng koos praktiliste näidetega. Õppematerjali juurde on koostatud koolitaja jaoks juhend (Lisa 4), kus on toodud välja koolituse sisu, medtoodika, piirangud ja kuidas õppematerjali kasutada. Valminud õppematerjalid saadeti hindamiseks eksperthindajatele, kellelt saadi hinnangud õppematerjali jõukohasuse kohta kutsekooli õpilastele ja kas see annab antud teemast ülevaate. Hinnati veel õppematerjali seostatust, struktuuri, arusaadavust, loetavust, kui otstarbekalt on selgitatud, kas teemade tähtsus on hästi väljatoodud ja kas õppematerjaliga saavutatakse õpieesmärgid. Teises osas tõid eksperthindajad välja, mis oli õppematerjali juures positiivset ja negatiivset ning mida peab muutma ja täiendavad nõuanded. Vastavalt ekspertidelt saadud tagasisidele muudeti sisu ja struktuuri ja parandati õppematerjalis olnud vead.

Valim

Intervjueeritavad peavad vastama kindlatele kriteeriumitele. (Laherand, 2008) Autori jaoks oli oluline, et intervjueeritavatel oleks antud temaatikaga isiklikke kogemusi ning pikk erialaline töökogemus. Ühendust võeti viie eksperdiga, kellest kolm andsid nõusoleku uuringus osalemiseks. Nendest kaks töötavad haridusasutuses, mis pakuvad kutseharidust või kõrgharidust ning üks töötab riigikaitsesvaldkonnas küberkaitse erialal. Kõikide ekspertide töökogemused antud valdkonnas on vähemalt neli aastat ja nad teevad oma tööd ka rahvusvahelisel tasemel. Seetõttu on need eksperdid pädevad antud teemal oma arvamust avaldama. Riigiametnike kaasamine antud uurimustöösse on vajalik, kuna küberkaitse on

muutunud oluliseks osaks riigikaitses ja noortes huvi tekitamine antud teema vastu on oluline järelkasvu vaatevinklist.

Küberekspertide eksperthinnangute jaoks lähtus autor valimi koostamisel mitmest asjaolust. Esiteks oli autorile oluline valdkonna sügav tundmine ja teiseks eksperdi pedagoogiline taust. Kokkuvõttes andis oma eksperthinnangu õppematerjalile (LISA 3) kaks eksperti Tallinna Tehnika Ülikoolist.

Andmete kogumine ja analüüs

Töös kasutati andme kogumiseks temaatilist poolstruktureeritud intervjuud (Lisa 1), jättes intervjuu käigus võimaluse lisaküsimusteks ja aruteluks. (Laherand, 2008) Autor soovis uurida, missugused on küberkaitseekspertide soovitused õppematerjali koostamisel kutsekooliõpilastele. Antud teema vajab paindlikku lähenemist, kuna küberkaitseeksperte on vähe ja nende tase ja kogemused on erinevad. Küsimustikud (Lisa 2)saadeti mõni päev enne intervjueeritavatele, et nad saaksid ennast intervjuuks häälestada ja läbimõeldud vastuseid anda. Vajadusel esitati lisaküsimusi. Intervjuu järel anti küberkaitseekspertidele võimalus antud vastuseid või teemat täiendada. Intervjuud toimusid 2017 aasta detsembris ja 2018 aasta jaanuaris nende poolt valitud kohas ja ajal.

Intervjuud lindistati digitaalselt kahe seadme poolt ning hiljem transkribeeriti. Jälgiti transkribeerimisnõudeid (Laherannale, 2008) ja rääkija kõne pandi kirja võimalikult täpselt. Intervjuu salvestamiseks kasutati programme Microsoft Corporation Kõnesalvesti ja Voice Recorder, nendega kuulati hiljem salvestusi, mille käigus tekst transkribeeriti *Microsoft Wordi* programmi abil. Salvestisi kuulati korduvalt ja kontrolliti transkribeeritud teksti ning tehti parandusi. Transkribeeritud teksti oli kokku 22 lehekülge.

Intervjuu transkribeerimisele järgnes kodeerimine. Intervjuuküsimuste vastused töödeldi programmi *Microsoft Wordi* programmi abil. Transkribeeritud tekst jagati osadeks ja loodi erinevad kategooriad, alamkategooriad ning koodid (Tabel 1). Analüüsi käigus vaadati üle ja muudeti kategooriaid ning koode koostöös küberkaitseeksperdiga.

Tulemuste osas on kasutatud uuringus osalenute tsitaate analüüsi ilmestamiseks. Konfidentsiaalsuse tagamiseks intervjueeritavate nimesid ei kasutata, neile anti koodnimed E1, E2 ja E3.

Eksperthinnangute saamiseks kasutas autor ankeetküsitlust (vt lisa 2), mille koostamiseks kasutati käesoleva töö käigus koostatud õppematerjali ning küberekspertide intervjuudest saadud andmeid. Tagasiside käigus uuriti, kuidas küberkaitseeksperdid hindavad koostatud õppematerjali, kas ja kuidas oleks vaja õppematerjali täiendada või parandada. Paluti välja tuua positiivsed ja negatiivsed küljed. Tagasiside lehed saadeti eksperthindajatele e-posti vahendusel.

Tulemuste osas on kasutatud tagasiside andnute tsitaate analüüsi ilmestamiseks. Konfidentsiaalsuse tagamiseks eksperthindajate nimesid ei kasutata, neile anti koodnimed EH1 ja EH2.

Tulemused

Küberkaitseekspertide arvamused küberkaitsealaste teadmiste ja oskuste kohta.

Küberkaitse meetmed.

Esimene peakategooria küberkaitse meetmed jagunes kolmeks alamkategooriaks: 1. ohud (pahavara, õngitses- ja petukirjad, võltsveebilehed, sotsiaalmeedia, identiteedi vargus, andmete lekkeleke, kelmused, küberkiusamine, sõltuvused ja tervisehäired), 2. käitumine (info jagamine, isikliku info kasutamine, töö ja eraelu lahusus, jalajälg, usaldus ja privaatsus) ja 3. seadusandlus (andmekaitse ja intellektuaalomand). Tulemused on järgnevalt esitatud vastavate alamkategooriate kaupa.

Ohud. Intervjuudest selgus, et kutsekooli õpilastele tuleb õpetada enamlevinuid ohte, saamaks aru, milles need seisnevad, kuidas see neid mõjutada võiks ja kuidas need toimivad.

> *(...)põhimõtteliselt nad võiksid aru saada millega tegu, kuidas sellesse suhestuda, kuidas nemad sellega puutuvad kokku puutuvad, kuidas nemad sellega seotud on ja kuidas nende elu ... elu mõjutada võivad nagu näiteks isikliku teabe paljastamine, isiklike andmete lekkimine, näiteks krediitandmete kaardi vargus (...)* E3

> *(...) sa pead tundma reegleid, sa pead oskama nii öelda ohtu hinnata, sa pead tegema ja pöörama tähelepanu noh nii öelda korralikule õigele käitumisele ja misiganes normidele ja muudele asjadele (...)* E3

Ekspert E3 tõi välja, et noortel on vaja kursis olla ohtudega, mis neid igapäevaselt küberruumis varitsevad või mis tulenevad arvutite kasutamisest. Nendeks ohtudeks võivad olla kõik ohud, mida interneti otsinguga leida võib.

> *(...)täiesti inimese poolt looduna täiesti tehislik maa, eee teda tema nii öelda tuumik koosneb ee nullidest ja ühtedest, mis tähendab seda, et kõike mida saab teha, kõike mida fantaasia suudab ette kujutada saab selles ruumis, sellele ruumile kehtivate reeglite alusel luua, kustutada, hävitada, mida iganes seal nagu piiranguid kui selliseid ei ole. Piirangud kehtestab ja seab piiranguid lõhub inimene ise.*

Ekspert E2 kirjeldas, mis teadmatus ohtudest ja nendega mitte arvestamine võib kaasa tuua peale selle, et langetakse ise kuriteo ohvriks või selle, et võib jääda süüdi kuriteos mida ise ei sooritanud.

> *(...)et sa võid küberkuritegevuse ohvriks langeda, mingisugusel viisil, sa võid kaotada oma identiteedi, raha ja kõik muud. Et just teadmatusest juhtub sinuga asju, mis, noh sa langed ise kuritegevuse ohvriks või sa jääd kaudselt kuriteos süüdi, sest kasutatakse sinu seadmeid või identiteeti.* E2

Vanemate, kui 45 aasta vanuste õppijate kohalt tõi ekspert E2 välja, et ka nende teadmised turvalisusest on kesised, nad on väga ettevaatlikud aga samas on nad koolitustel julged küsima ja uue informatsiooni suhtes avatud. Ekspert E1 tõi välja, et ka õpetajatel on puudu küberkaitsealastest baasteadmistest ja see mõjutab ka nende tööd õpilastega. Näitena toodi see, et arvutitesse ei logita oma kasutajaga sisse, vaid kas siis õpetaja või teine õpilane logib sisse oma andmetega.

> *Täiskasvanutel on, kui rääkida 45pluss inimestest, siis nendel on ikkagi nagu väga võõras kõik mis puudutab turvalisust ja nad noh nad on väga ettevaatlikud, mis on positiivne. Selles mõttes nad kardavad ja kahtlustavad kõike, aga samas nad ei oska teha õigeid valikuid, kui tuleb mingisugune asi, mis neid isiklikult puudutab, siis nad ei oska sellele reageerida, täpselt nagu need petukirjad, et keegi kuskil hädas ja nad päris täpselt ei tea mida teha (...)* E2

Kõik eksperdid tõid välja selle, et õpilastel peab tekkima isiklik seos, kuidas see neid endid võib puudutada.

> *(...) neid huvitavad need asjad just sügavuti, kui see võib neid isiklikult puudutada (...) E2*
>
> *Ma arvan, et just see baasiline küberhügieen, kuidas ennast kaitsta, just see, et kuidas see seostub minu endaga, neil ei ole vaja nii palju selliseid üldisi asju, muidugi hea teada ka, et meil on sellised võimalused Eestis ja tehakse seal x-teed muud asjad ja aga noh pigem just, kuidas on võimalus ise ennast kaitsta, mis võivad olla need ohud endale.* E2
>
> *No ja teine asi, mis on seal juures oluline, kui rääkida erialadest, et kui nad kuhugi lähevad tööle, et siis tööandja ja isikliku... ja noh töö ja isikliku asja lahus hoidmine, et see on ka üks turvalisuse risk tihtipeale.* E2

Enamlevinud ohtudena, mida algtasemel teada võiks, toodi välja pahavara, identiteedi vargus, andmevargus, ohud sotsiaalmeedias, küberkiusamine, igasugused kelmused ja õngitsus- ning petukirjad mille ohvriks võib langeda ning.

> *(...) küsitakse aga mis see identiteedivargus on, mis see mulle tähendab, miks ta ohtlik on, so what keegi võtab mu nime ja isikukoodi, mis ta saab sellega teha, selliseid asju tahetakse teada.* E2
>
> *(...) lihtsalt igasugused teadmised küberohtudest, et mis neid ennast võivad ohustada, lihtsalt inimesed ei tea, et identiteedivargus või andmevargus või sotsiaalmeedia, mida sa võib teha, mida sa ei või teha, mida see tähendab või see.* E2
>
> *Ja siis igasugused kelmused, mille ohvriks võib langeda, nii nutikad juba tänapäeval.* E2
>
> *(...) siis tingimata on see interneti puhul on kõik need võtlssaidid „fishingud" siis on see sama, et kas ma linkide peale klõpsan või ei klõpsa (...)* E1

> *(...)sotsiaalmeedias mida ma teen, mida ma ei tohi teha, mida ma võin jagada ,kuidas ma jagan, (...) kui ma kuskile video ülesse panen, et mis õigustega ma panen (...)*E1

Ekspert E1 rõhutas tähelepanelikkuse vajadust, näiteks veebilehtede juures, kas osatakse jälgida ja vaadata kas ollakse veebilehel, mida soovitakse külastada või on tegu võltsveebilehega.

Ekspert E2 tõi välja ka selle, et vähe pööratakse tähelepanu terviseprobleemidele nii füüsilises kui ka vaimses mõttes ja sõltuvustele. Internetist on lihtsalt kättesaadavad online kasiinod või lihtsad mängud mis võivad tekitada probleeme sõltuvusega. Lisaks kulutavad noored palju aega suhtlemisele sotsiaalmeedias (Facebook, instagram jne) ilma milleta enam olla ei saa.

> *Ja üks asi, millest ka väga palju ei räägita, mis otseselt ei ole küberhügieen aga kaudselt on, on terviseprobleemid ja siis sõltuvuse probleemid, neid on teatud määral juba uuritud ka aga neid eriti ei kajastata kusagil.* E2

<u>*Käitumine.*</u> Intervjuudest selgus, et noortel on vaja kursis olla turvateadliku käitumisega ja seeläbi osata hinnata ka ohtusid.

> *(...) on neil vaja teada käitumist, kuidas kuidas kuidas käituda turvaliselt, millele tähelepanu pöörata, laia võtmes nad võiksid osata ka, kuidas öelda siis, hinnata ja ette näha ohu olukordasi, mitte ainult enda vaid ka teiste puhul, teiste käitumises. E3*

Probleemiks toodi noorte teadmatuse ja asjades kogenematuse, kuidas noored ennast ise ohustvad. Nad ei oska arvestada, et nende tegemised ja postitused internetis jäävad sinna pikaks ajaks ning see võib neid mõjutada olulisel määral tulevikus.

> *Nii öelda sinu jalajälg jääb kestma aastateks, et mis see võib tulevikuks kaasa tuua. Ja siis info jagamine sama asi, et noh mida sa võiksid jagada mida mitte nii viisi, pilte üles panna, millist infot enda kohta jagada.* E2

> *Või siis tulevikus ei saa kuskil tööd, sest sa kuskil 5 aastat tagasi, midagi kuskile postitasid. E2*

Hiljem kui minnakse erialasele tööle siis tööandjate juures tehakse viga sellega, et ei hoita isiklikud ja tööalaseis asju lahus, näiteks töö email kasutamine isiklike asjade ajamiseks.

> *No ja teine asi, mis on seal juures oluline, kui rääkida erialadest, et kui nad kuhugi lähevad tööle, et siis tööandja ja isikliku... ja noh töö ja isikliku asja lahus hoidmine, et see on ka üks turvalisuse risk tihtipeale.* E2

Eksperdid suunasid tähelepanu, sellele, et inimestest endist ja nende käitumisest sõltub suuremosa turvalisusest. Millist informatsiooni jagatakse, kuivõrd usaldavad nad on ja kui palju pööratakse tähelapanu privaatsusele.

> *Ja see ongi, palju sõltub sinust endast, enamus asju sõltub sinust endast, sa ei pea üldsegi kutsuma mingi IT poisi alati kui on mingi probleem.* E2

<u>*Seadusandlus.*</u> Intervjuudest selgus, et seni on vähe tähelepanu pööratud õigusalaste teadmiste õpetamisele, intellektuaalomandile või erinevatele eeskirjadele ja nõuetele. Õpilastele on vaja selgitada näites, mis vanusest võib omada Facebook'i kontot, kas teatud pilte võib saata või kasutada jne.

> *(...) seletama lahti seaduseid, (...) aga need seadused samad, nii noh need samad, mis vanuses Facebooki teha, kui sa teed, kas ma võin mingiseid teatud pilte saata või ei või või sellised asjad.* E1

> *(...) kuidas ma kasutan kellegi teise asju, kas ma võin neid kasutada, kas ma pean viitama, kuidas viitamine võiks käia, (...)kõik need kaubamärk ja litsentsid ja siuksed asjad ja bränd (...) intellektuaal omandi ja selle seadusega seoses (...)* E1

<u>Praktilised teadmised.</u>

Teise peakategooria praktiliste teadmiste alla kuulub kuidas ennast kaitsta (viirusetõrje, tulemüür, varundamine, turvaline veebileht HTTPS, kust ja kuidas otsida, kus ja kuidas seadmeid kasutada, paroolid ja turvaline ühendus VPN) alamkategooria.

Kõikide ekspertide arvates on noortele vaja anda praktilisi teadmisi, mida nad saavad igapäevaelus kasutada. Näiteks milliste meetoditega saab oma seadmeid kaitsta viiruste eest, kuidas oma seadmes olevaid programme uuendada, milliste vahenditega saab turvaauke lappida. Õpilased peaksid teadma mis on tulemüür ja kuidas seda kasutada, mis on turvaline ühendus e VPN.

> *(...) et nad teaksid mis asi on antiviirus, mis asi on uuendus, mis asi on paikamine, mis asi on tulemüür jne jne ja mille jaoks neid vaja on ja mis on mm milles peitub nende efek (...)* E3

Oma oluliste andmete säilitamisel tõid eksperdid välja andmete varundamise, kuhu ja millal varundada ning mis on selle eesmärk. Näitena toodi oluliste failide kaotsimineku, mis võib tuua rahalist kaotust, kui ka hindamatut kaotust.

> (...) *mida ma olen näinud et varundamine, varundamine on kõige nõrgem koht nendel ja see nad unustavad hästi tihti ära kuhu ma mingi asja panin.* E1

Noortel on puudu praktilistest teadmistest, mis on seotud turvalise veebilehega (https) ja kust ning kuidas otsida. Ekspertide arvates tuleb anda neile teadmised, milliseid ettevaatus abinõusid nad peaksid rakendama, kui nad kasutavad kellegi teise arvutis internetti.

> *(...) mida ma seal internetis teen, eraldi internetis googeldan, kuidas ma googledan, kas ma seal firefoxis või Google chromes kasutan mis ta on nüüd, mis moode ta on inkognito, kui ma olen kuskil teises arvutis, siis ma kasutan seda, (...)* E1
>
> *Et nad klikivad hea meelega igale poole kuhu saavad ja ja nad suht tihti ei mõtle mis selle taga on ja noh taust teadmisest on nii palju puudu, et nad ei oska seoseid luua enam turbe, turvalisuse ja tarbimise vahel (...) E3*
>
> *(...) ei suuda informatsiooni leida (nad ei oska Google't kasutada) nad oskavad aga nad selles mõttes ei oska sorteerida informatsiooni nagu nii moodi. Nad käivad esimese lehekülje läbi, kui esimese kahe kolme juures, nad võtavadki kahe esimese kohe asja nagu tõepähe, nad ei hakkagi mõtlema, et loeks rohkem informatsiooni läbi (...)* E1

Ühe tavalise probleemina toodi välja paroolide ja salasõnade hoidmise ning säilitamise olulisuse, kui ei suudeta seda meeles pidada. Erinevates kohtades tuleb kasutada erinevaid paroole ning vältida tuleb nende ristkasutust. Ei teata ega kasutata parooliga sisenemise asemel kahesüsteemset audentimist mis on oluliselt turvalisem.

> *Muidugi ka täiesti elementaarsed asjad nagu salasõnade hoidmine (...)* E2
>
> *(...) siis kasutada erinevaid salasõnasid, täpsemalt välja tuua mis on põhjus, miks tuleks kasutada, kas on valid erinevaid variante, et kui parooli kasutada kahe korra audentimist või mobiiliga või millega, et need võiks kõik välja tuua (...)* E1

<u>Praktilised oskused.</u>

Kolmas peakategooria praktilised oskused jagunes seitsmeks alamkategooriaks: 1. tarkvara (tarkvara jms laadimine ning kasutamine, ajakohasus ja päritolu), 2. seadmed (seadmete kasutamine, esmane seadistamine, turvaseaded, kasutajad, kontroll, puhastus, jagamine ja seadme lukustus), 3. uuendused (kontrollimine, paigaldamine ja seadistamine), 4. varundamine (kuidas, kuhu, turvalisus ja krüpteerimine), 5. internetis liikumine (mida kasutada, kus kohast otsida, kuidas otsida ja jagamine), 6. parool (hoidmine, moodustamine, kahesüsteemne audentimine ja parooli vahetus)ja 7. ID-kaart (kasutamine, uuendamine ja krüpteerimine). Tulemused on järgnevalt esitatud vastavate alamkategooriate kaupa.

Ekspert E3 tõi üldiselt välja selle, et noortel on vaja üldiseid praktilisi teadmisi ja oskuseid mida on vaja igapäevatoimetuste juures, kui kasutavad arvuteid ja internetti.

> *No hästi ümmargune vastus on see, et neid oskusi teadmisi, mis on seotud igapäevase küberkäitumisega, ehk siis käitumisega interneti maailmas infotehniliste vahenditega ja kõige sellega, millega nad nii öelda küber võtmes kokku puutuvad.*

Tarkvara. Ekspertide hinnangul ei pöörata tähelepanu tarkvara päritolule, ei teata, kuidas ja kust on turvaline oma seadmesse programme laadida. Hilisemal kasutamisel ei jälgita selle ajakohasust, ega tehta uuendusi.

> *(...) kuidas mida kuskilt alla laadida, mida mitte, millised on võimalused ennast kaitsta (...)* E2

Seadmed. Eksperdid märkisid, et praktiliste oskustena on puudu oskustest, mis aitaksid seadmeid turvaliselt käsitseda, sealhulgas esmane seadistamine ja erinevate turvaseadistuste kasutamist ning vahenditest. Erinevate võimalustena, mis muudavad elu turvalisemaks, toodi välja see, et arvutit ei pea kasutama administraatori õigustega vaid igapäevaselt võib seda kasutata tavakasutajana. Igapäevaste praktiliste oskustena toodi välja seadmete kontrolli ja puhastamise.

> *(...) ID-kaardid, mobiil ID ja lihtsalt arvuti puhastamine, korrastamine, hindamine, mis on õige, mis ei ole ja isegi kui arvutiga juba osatakse natukene midagi teha, siis nutiseadmed on need, mille puhul ei osata eriti midagi üldsegi teha, turvalisuse mõttes. Et eeldatakse, et sa saad selle telefoni siis kõik väga turvaline, seadistatud, ei ole vaja üldsegi muretseda selle pärast.* E2

> *(...) mis õigustes ma arvutis sees käin, kas ma olen administraatori õigustes või mul on kasutaja õigused (...)* E1

Elementaarse probleemi seadmete kasutamise juures tõid eksperdid välja selle, et seadmetest ei logita välja ega lukustata neid. Seeläbi tekib teistel ligipääs nende asjadele ja võimalus kas siis nalja teha (saata kõigile kiri), kurjalt ära kasutada (andmevargus) või põhjustades hindamatut kahju (tööde kustutamine).

> *(...) esimene asi see, arvutitesse sisse logimised välja logimised, arvuti lukku panek. See on meie kooli baasil on näha et õpilased unustavad ära selle, et nad peaksid selle arvuti lukku panema või miks ma peaksin lukku panema.* E1

Uuendused. Tingimata peavad ekspertide arvates õpilased olema kursis tarkvarale uuenduste tegemisega (kontrollimine, paigaldamine ja seadistamine). Arusaamine miks ja mis põhjusel neid vaja teha on vaja, ajakohased uuendused hoiavad ära vananenud tarkvarast tulenevad ohud.

> *Uuendused, et miks on vaja neid uuendusi teha, mis on selle põhjus (...) et uuendusi nad võibolla teevad kui see automaatselt käib (...) või et siis nad lasevadki kõik uuendused läbi, nad ei mõtlegi (...)* E1

Internetis liikumine. Üldine soovitus ekspertide poolt oli õpetada ja anda teadmisi internetis liikumise ja seal käitumise kohta. Tihtilugu piirduvad noorte teadmised ainult rakenduste ja seadmete kasutamises, st näiteks nutitelefon on helistamise ja sotsiaalmeedias suhtlemiseks või e-kirjade lugemiseks. Nad ei oska või ei taha pöörata tähelepanu turvalisusele, mis on näiteks seotud seadmete kasutamise või internetis liikumise puhul.

> *(...)selles suhtes, et inimesed üldises laastus teavad, mis on Facebook. Nad oskavad seda kasutada, nad oskavad teiste inimeste pilte vaadata, nad oskavad neile hindeid anda, no seal on küll pöial üles pöial alla, ja nad oskavad kommenteerida. Aga väga valdav osa, suurem osa, nii öelda ei tule selle peale, et seal võiks rakendada kahesüsteemilist autentimist, et seal on olemas nii öelda, noh inglise keeles öeldakse token, nii öelda lisavahendiga autentimine ja igast muud viisid kuidas kaitsta oma kontot selle eest, et seda üle ei võeta. Pluss siis veel kaitsta oma teavet selliselt, et seda ei saaks keegi teine kuritarvitada ja seda ei näeks terve maailm (...) nad on sellised tarbijad, kes tarbivad aga neid see muu kuidas mismoodi milleks see kõik nendeni jõuab ei huvita. Neid ei huvita ka turvalisus kahjuks.* E3

> *Et ole tähelepanelik, et vaata kus sa käid, (...)* E1

Interneti kasutamine on tänapäeva noortel juba elu lahutamatu osa. Seal veedetaks niisama aega või suheldakse sõpradega. Samuti kasutavad koolid oma õppetöös palju internetti, arvuteid või nutiseadmeid, õppetöö on muutunud interaktiivsemaks. Oluliseks peeti ka kuidas, mida ja kellele jagatakse ning sellest tulenevad ohud. Ilma mõtlemata sisestatakse oma andmeid mida küsitakse.

> *IT õpilased kellega olen kokku puutunud kasutavad internetti no väga palju õppetööks, teised kasutavad nii nagu kõik noores sotsiaalmeedia, ee… siis kirjavahetus, uudised ja muud sellised. Õppetööks kasutatakse ikka ka.* E2

> *(...)käin igal pool, ma, ongi see, et ta läheb võtab lehekülje lahti, surfab, ta käib igal pool ja nagu ei mõtlegi kuhu ta klikib, et hästi palju nad mängivad, kui keegi soovitab siis nad lähevad sinna lehele, nad ei mõtlegi selle peale, igale poole panevad oma infot.* E1

ID-kaart. Ekspertide arvates on õpilastele vaja õpetada ja selgitada ID- kaardi olemust ja selle kasutamise võimalusi seal hulgas krüpteerimist.

Küberkaitseekspertide arvamused õppematerjali ülesehituse ja sisu kohta.

Õppevahendi ülesehitus.

Kategooria õppevahendi ülesehitus jagunes kolmeks: 1. teooria, 2. vastumeetmed ja 3. praktilised ülesanded.

Üks ekspert pidas oluliseks koolituse alguses teostada teadmiste kontrolli saamaks teada koolitatavate taset ja tausta ning edasi liikuda sissejuhatava loenguga. Peale sissejuhatavat loengut minna terminoloogia ja meetodite juurde.

> *Et ma alustan alati reeglina siukest ülevaatlikust, sissejuhatavast loengust, kus ma püüan aru saada milline mis publik mul on, siis sealt edasi ma liigun ee sihukesele seletavale terminoloogilisele seletajale, seletan mis mis ründed on, mmm mis meetodid on, eee toon näiteid elust enesest, kui võimalik siis seon näited erinevate videotega, võtan natukese internetist, või siis natuke populaarsemate teemadega.* E3

Kõik eksperdid tõid välja, et iga teoreetilise osa järel peab tegema asjad praktiliselt läbi. Harjutused peaksid olema võimalikult ligilähedased reaalsele elule ja seotud näiteks selle valdkonnaga, millega on seotud õpilased, kes tunnis osalevad.

> *(...) et tõesti ta peab mingisse otsuse tegema nagu ta elus peab tegema ta mingisse otsuse tegema ja peab tulema tagajärg et näe et kas see et kas sul läks hästi see asi, tegid õige otsuse ja nüüd ole hea ja mõtle, mis see õigesti on (...)* E1

(...) paroolide puhul võib täiesti olla see, et pikk nimekiri paroole ja nad peavad näiteks linnutama milline nad arvavad, et siis oleks nagu kõige parem parool (...) E1

<u>Õppevahendi sisu.</u>

Õppevahendite sisu kategooria jagunes kolmeks alamkategooriaks: 1. küberkaitse meetmed (mis, milleks ja praktilised harjutused) 2. Praktilised teadmised (näited, kirjeldused ja praktilised harjutused) 3. Praktilised oskused (näited, kirjeldused ja praktilised harjutused otsustus mängude ja muude samalaadsete mängude abil).

Ekspert E3 tõi välja, et õppematerjali sisu peab olema praktiline.

> *No õppematerjali sisu peaks olema praktiline noh et jah seda on kerge öelda.* E3
>
> *(...)et inimene õpib kõige paremini kuuldes, nähes ja tehes (...)* E3
>
> *Et tal tekivad seosed ja ta seostab neid asju, et tal tuleb meelde et midagi tuttavat toimub, et ta oskab seda nagu adresseerida.* E3

Praktiliste harjutuste osas soovitati juba olemasolevaid internetipõhiseid vabalt kättesaadavad otsustusmänge või keskkondi, kus saad ise luua oma teste ja harjutus.

> *(...) hotpotatosil on see et sa saad siukseid ülesandeid siin teha (...) saad ära märkida, et näe see on õige, see on vale jah no ta teeb automaatselt ja sulle tuleb ka see tagasiside (...)* E1
>
> *(...)peab olema tõesti mingised ülesanded, mingised ülesanded kasvõi see, et juhtumid, (...) välja toonud mingised case´id, kus (...) välja tooma mis oli see probleem, kuidas*

lahendati, kuidas sina lahendaksid , kuidas oli võimalik seda tõestada ja sellised asjad, tõesti, et juhtum, kui ta oleks tõesti elust endast võetud juhtum(...) E1

Eksperthinnang õppematerjali kohta.

Eksperthindaja EH2 oli täiesti nõus, et antud õppematerjal on kutsekooli õpilastele jõukohane ning eksperthindaja EH1hindas seda nii ja naaks. Õppematerjali osade omavahelise seostatuses hindas eksperthindaja EH1 pigem heaks, kuid eksperthindaja EH2 ei olnud nõus, et osad on omavahel hästi seostatud. Õppematerjali loetavuse hindas eksperthindaja EH1 pigem heaks ja eksperthindaja EH2 hindas selle nii ja naaks. Õppematerjali struktuuri selguse hindas eksperthindaja EH1 pigem heaks aga eksperthindaja EH2 hindas selle nii ja naaks. Eksperthindaja EH2 oli pigem nõus, et õppematerjalis kasutatud laused on arusaadavad, eksperthindaja EH1 hindas seda pigem heaks või nii ja naa. Õppematerjali sisu otstarbekat selgitust hindasid mõlemad eksperthindajat nii ja naaks. Kas õppematerjali sisu annab antud teemast ülavaate, hindasid mõlemad pigem heaks. Sellega, et õppevahendi teemade tähtsus on hästi ära näidatud, oli eksperthindaja EH1 täiesti nõus aga eksperthindaja EH2 hindas selle keskmiseks. Antud õppematerjaliga, eksperthindaja EH1 arvates, võib saavutada keskmised õpieesmärgid ja eksperthindaja EH2 oli sellega väitega pigem nõus.

Eksperthindaja EH1 hindas õppematerjali juures eriti positiivseks soovitusi mis on õppematerjali lõpus. Positiivseks hindas ta ka ühtset struktuuri ja teemasid millega tavainimene võib kokkupuutuda.

"Välja on toodud tehnilisemad teemad, millega tavainimene võib kokku puutuda digitaalse ohutuse ja küberkaitse valdkonnas. Ohte on püütud analüüsida ühtse struktuuri alusel (kirjeldus, päritolu, tuvastamine, eemaldamine ja ennetamine). Eriline väärtus on soovitustel kõige lõpus." EH1

Eksperthindaja EH2 tõi õppematerjali juures välja positiivsena selle, et see katab nii tehnilisi kui mitte-tehnilisi ohte ja probleeme ja annab soovitusi probleemidega toimetulemiseks.

- *Katab nii tehnilisi kui mitte-tehnilisi ohte ja probleeme.*
- *Annab soovitusi probleemidega toimetulemiseks.* EH2

Negatiivseks hindas eksperthindaja EH1 seda, et teatud teemad vajavad süvendatumat lähenemis või pikemaid tutvustusi kommentaarides, kui töö autor seda tegi. Lisaks puudusena toodi välja, et ei järgitud üldstruktuuri vastavalt sisukorrale ning eines kirjavigu.

“Kirjavead, osad slaidid vajaks pikemat tutvustamist „märkmetes“, struktuur ei järgi sisukorras antavat loogikat täies mahus ja osad teemad vajaksid pigem sügavamat lähenemist (praktilist poolt) et muuta käitumist. Kuna eesmärgiks on info esmane jagamine, siis ma ei loe praegu slaididest välja kui sügavikuti teemasse sooviti minna ja mindi bakalaureusetöös endas.” EH1

Negatiivsena tõi eksperthindaja EH2 välja, et ülesehitus oli segadusse ajav, kuna esines ebaloogilist järjestust ning esines ebatäpsust ja keelelisi vigu.

- *Mõned ebatäpsused ja keelelised vead.*
- *Sisemine organisatsioon ebaloogiline. Hetkel on järjekord segadusseajav, kuna tuleb pahavara, kiusamine, siis jälle pahavara, siis social engineering ja identiteedivargus, siis turvaaugud ja siis petuskeemid. Soovitaks loogilisemat ülesehitust, nt. kõigepealt tehnoloogilised probleemid ja siis „pehmed“ probleemid vms.* EH2

Õppematerjali juures võiks muuta eksperthindaja EH1arvates seda, et enne ja pärast koolitust võiks toimuda teadmiste testimine, ning kogu õppematerjal võiks olla kompaktsem.

“Teemasid saaks esitada kompaktsemalt. Praktiline/kaasav osa võiks anda lisaväärtuse (nt. test enne/pärast), mis toimib eelhidamise ja järelhindamisena. Slaidi kasutaja võiks vajada lisaabi sisu selgitamisel (tunnikava, abijuhis või detailsemalt koostatud „märkmed“ vms). Slaidide alguses võiks tuua välja fookusgrupi ja õpiväljundid.” EH1

Eksperthindaja EH2 tõi välja vajalike muudatustena kattuvate ja sarnaste slaidide kokkuviimise, andis nõu, kuidas sisulist poolt täpsustada, tõi välja eksimised terminites ja soovitas lisaülesannet.

“6: tuleks teha vahet ohtudel ja turvanõrkustel

6: pahavaral ei ole eesmärki, pahavara kasutajal on;“ EH2

“12: pahavaranakkuse ennetamiseks on soovitatav ka viirusetõrjeprogrammi kasutamine“ EH2

“16: lisaks veel: sotsiaalmeedia- või meilikonto on üle võetud (ei saa sisse, parool muudetud); lisandunud on uusi programme/äppe; lisandunud/kadunud on mingeid faile; muutunud on arvuti seaded (nt sisendkeel), jms. Samas, kavalama pahavara puhul kergestimärgatavaid tundemärke ei ole. “ EH2

“26: troojalane ei pruugi olla maskeeritud programmiks vaid võib ennast „näidata“ ka mõne andmefailina (nt. Excel ,pdf, jne). “ EH2

“86: mis on kettadraiv?

95: +1 ÜL: päiste edastamine.

100: täita või kustutada” EH1

Täiendava tähelepanekuna tõi eksperthindaja EH1 välja lisamaterjali lisamise ja praktiliste ülesannete väljatöötamise vajaduse.

> *"Slaidid võiks toimida ühtse komplektina, et ei oleks vajadust lugeda lisamaterjali. Või peaks olema viide lõputööle, millest lisamaterjali lugeda. Praktilised harjutused, mida viidatakse oleks väärtuslik lisa tulevikus."* EH1

Arutelu

Käesoleva bakalaureusetöö eesmärk on uurida, et millised küberkaitsealased teadmised ja oskused on vajalikud kutsekooliõpilastele küberkaisteekspertide arvamuste põhjal, milline peab olema õppevahendi ülesehitus ja sisu ning kuidas hindavad küberkaitseeksperdid koolitusmaterjali sisu ja vajalikkust. Käesolevas peatüki alguses arutletakse üldiste tähelepanekute üle ning peatüki teises pooles arutletakse tulemuste üle uurimisküsimuste kaupa.

Käesoleva uurimuse raames tõid küberkaitseeksperdid välja teema vajalikkuse ja leidsid, et küberkaitsealaseid algteadmisi tuleb õpetada kõigile sõltumata vanusest või erialast. Samale järeldusele jõudis, ka Sulo Seim 2013. a oma lõputöös. Kuid üldise probleemina toodi esile, et IT ja IKT õpetajate koormus oma valdkonnas on suur ja nad ei jõua õpetada ka teiste eriala valdkonna õpilasi. Teistel erialadel peale ITK eriti küberkaitsealaseid baasteadmisi ei õpetata, mõningaid teadmised ja oskused võivad küll lõimitud olla teiste ainete, oskuste või teadmistega. Ühe ettepanekuna tehti, et võiks leida võimaluse, kuidas saaks küberkaitsealaseid algteadmisi anda kõigile sõltumata erialast. Soovitati otsida ühiseid aineid või teemasid mille kompetentsi sellised teadmised ja oskused võiks kuuluda või kuhu siduda. Samas kutsehariduss tandard kirjeldab, milline infotehnoloogiline pädevus peab olema erinevatel kutseõppe tasemetel, näiteks teab infotehnoloogia peamisi võimalusi ja potentsiaalseid ohte. Infotehnoloogiline pädevus on suutlikkus kasutada oskuslikult ja kriitiliselt infotehnoloogiavahendeid ja digitaalmeediat. (Vabariigi Valitsus. 2016) Antud töö raames seda võimalust ei uuritud, aga teema on oluline ja vajab edasiuurimist.

Üks ekspert soovitas enne koolitust või koolituse alguses teha kindlaks õpilaste teadmiste taseme, see annab õpetajale võimaluse, kas siis osad teemad vahele jätta või mõnda teemat süvendatult anda. Lisaks soovitati õppematerjal teha interaktiivse ja luua veebipõhise õppematerjali, kuhu saaks järjepidevalt uut informatsiooni lisada. Selle teostamiseks kujunes oluliseks piiranguks see, et antud töö autoril puuduvad selleks vajalikud teadmised, oskused ja vahendid ning seepärast seda võimalust edasi ei uuritud. Õppematerjali koostamise juures on kasutatud “aju ühilduv õppimine” põhimõtteid, kus emotsioonidel rõhudes panna inimesed õppima. Selleks on kasutatud näitlikustavaid video lõike, mis võivad üllatada või tekitada hämmastust. Teise põhimõttena on anda kogemus ja näidata, kui oluline see tema jaoks on. Selleks on mõeldud praktilised ülesanded. Antud töös ei ole uuritud ja õppematerjali

koostamise juures ei ole välja töötatud praktilisi ülesandeid õpilaste jaoks, kuid edasiste uuringute või lõputööde käigus tuleks need luua.

Esimese uurimisküsimusega sooviti teada saada küberkaitseekspertide arvamuse põhjal, et missugused küberkaitsealaseid oskused ja teadmised on vajalikud tänapäeva noortele ning millistest teadmistest on puudu. Uuriti veel millised ohud tulenevad puudulikest teadmistest ja oskustest. Küberkaitseeksperdid loetlesid valdkonnad või teemad, mida tuleks kindlasti kutsekoolis õpetada. Selgus, et tänapäeva noortel on tihtilugu puudu elementaarsetest teadmisest, mis on seotud turvateadliku käitumisega. Noori peab harima nii, et nad oskaksid leida seoseid ja oskaksid ohte ennetada. Selle toob välja ka DigiTurvise (Lorenz, Laugasson, Püvi & Laanpere 2014) uuringu aruanne, et teadlikkust on vaja tõsta kõigi tasemete haridusasutustes, sest kübrkuritegevust saab ennetada tõstes üldist teadlikkust riskidest, see aitab ennetada ohtusid ja aitab ära tunda intsidente ning annab oskuse neile reageerida. Ka Riigi Infosüsteemi Amet suunas 2016. aastal oma tähelepanu ennekõike lõppkasutajate teadlikkuse tõstmisele, andes kodulehe ja sotsiaalmeedia kanalite kaudu praktilisi tegevusjuhiseid krüptolunavara vältimiseks, e-posti kontode kaitsmiseks ja sotsiaalmeedias varitsevate ohtude eest hoidumiseks. (Riigi Infosüsteemi Amet, 2016)

Uuringu tulemuste osas, töö teoreetilise osa ja ekspertide arvamuste osas oli erinevuseks, et eksperdid tõid välja võltsveebilehed, terviseprobleemid ja sõltuvuse, andmekaitse ja intellektuaalomandi, turvalise ühenduse VPN, praktiliste teadmistena kuidas ja kus erinevaid seadmeid kasutada, praktiliste oskustena tarkvara ja seadmete haldamise (allalaadimised, seadistamised ja teadmised päritolust) ja ID-kaartide kasutamist. Ekspertide antud soovitusi arvestati õppematerjali koostamise juures.

Teise uurimisküsimusega uuriti, milline peab küberkaitseekspertide arvates olema õppematerjali sisu ja ülesehitus. Intervjueeritavad eksperdid arvasid, et õppematerjali sisu peab sisaldama levinumaid ohte ja elementaarseid vastumeetmeid neile. Ülesehituse kohalt selgus, et kõik eksperdid soovitavad iga teoreetilise osa järel teha kohe praktiline harjutus või tegevuse läbimäng. See teeb tunni huvitavamaks ja kinnistab õpitut. Seda soovitust toetab ka "aju ühilduv õppimine", kus õppimisprotsessi ajal tuleb materjali esitada viisil, mis soodustab probleemide lahendamist ja kriitilist mõtlemist. (Reid, Niekerk & Solms 2011) Üks ekspert soovitas koolituse alguses ja lõpus teha teadmiste kontrolli, et aru saada mis tausta ja teadmistega on koolitusel osalejad ning seeläbi saab koolituse sisu valikul arvestada. Seda toetab ka Valentine (2006) ja Schultz (2004), nad toovad välja, et probleemiks on lähenemine, et ühesugune materjal sobib kõigile, arvestamata õppija eelnevaid teadmisi ja

oskuseid. Seeläbi võivad õppijad olla koolitusest pettunud, kuna nad ei õppinud midagi juurde. (Valentine, 2006; Schultz, 2004)

Kolmandas uurimisküsimuses uuriti, kuidas hindavad küberkaitseeksperdid koolitusmaterjali sisu ja vajalikkust. Eksperthindajad hindasid õppematerjali kutsekooli õpilastele jõukohaseks ja vajalikuks. Positiivsena tõi üks eksperthindaja välja praktilised soovitused. Selle tõi välja ka Schultz (2004), et inimestele võiks õpetada erialaseid teadmisi, mis nende igapäevaelus kasulikud ja rakendatavad on. Hinnangutest selgus puudustena ülesehituse osas, see tähendas, et esines kordavat informatsiooni (meetmed, ennetus jne) mida saab kompaktsemalt esitled. Õppematerjali mahu olulisuse tõi välja ka Mikk (2001), et väga mahukad õppevahendid ei arenda mõtlemist. Hiljem parandati ja täiendati, vastavalt eksperthindajate kommentaaridele, õppematerjali ülesehitust, muutes seda kompaktsemaks.

Võimalikeks probleemideks ja piiranguteks antud õppematerjali kasutamisel võivad olla keeleoskus, koolitusel osalejatel vähene tehniline kogemus, mille tõttu tuleb räägitavat selgitada. Keerulise teksti probleemi tõi välja ka Mikk (2000), liiga keeruline või lihtne tekst kasutamine ei pruugi anda uusi teadmisi, ei arenda mõtlemist ja on igav.

Kokkuvõte

Käesoleva bakalaureuse töö eesmärgiks on koostada väljaõppematerjal kutsekooli õpilastele lähtuvalt küberkaitsespetsialistide seisukohast, tõstmaks nende teadmisi arvuti igapäevase kasutamise ohtudest ning tutvustada abivahendeid isikliku info kaitsmiseks. Uuringus leiti vastuseid järgmistele uurimusküsimustele:

1. Millised küberkaitsealased teadmised ja oskused on vajalikud kutsekooliõpilastele küberkaisteekspertide arvamuste põhjal?
2. Milline peab olema õppevahendi ülesehitus ja sisu?
3. Kuidas hindavad küberkaitseeksperdid koolitusmaterjali sisu ja vajalikkust?

Küberohtude ülevaates ja õppematerjali loomisel on keskendutud rohkem tavakasutajale. Töös on pööratud tähelepanu enamlevinud võimalikele ohtudele nii minevikust, kui ka ohtudele, mis on muutunud järjest sagedasemaks. Töö teoreetilises osas antakse ülevaade küberkaitsealastest algteadmistest ja õppekirjanduse koostamise alustest lähtuvalt erialakirjandusest. Andmeid analüüsiti kvalitatiivse uurimuse meetodil temaatilise sisuanalüüsiga. Töö käigus valminud õppematerjalile hinnangu andnud küberkaitseeksperdi valim koosnes kahest eksperdist. Loodud õppematerjal võiksid olla abivahendiks kutsekooli õpetajatele või täiskasvanu täiendkoolituste läbiviijatele, kellele eesmärk on oma koolitatavaid harida ohtude suhtes, mis varitsevad arvuti igapäevase kasutamise juures ja teadmiste ning oskustega isikliku info kaitsmiseks.

Käesolevas töös läbi viidud uuringu tulemustena saab välja tuua, et enamlevinuid ohte internetis ja sotsiaalmeedias on palju, millele peavad tänapäeva noored tähelepanu pöörama, kui tahavad oma ohutust ja turvalisust tagada. Intervjueeritud eksperdid tõid välja, et noortel ja ka täiskasvanutel on puudujääke nendes teadmiste ja oskuste osas. Enamlevinud probleemi näitena toodi, nii õpilaste kui ka õpetajate puhul, arvutitesse sisselogimised ja väljalogimised. Andes inimestele teadmised ohtudest ja suuniseid ohu ennetuseks, on lootust, et nad muudavad oma igapäeva tegemised küberruumis turvalisemaks.

Eksperthindajad leidsid, et loodud õppematerjal on jõukohane kasutada kutsekooli õpilaste väljaõppes. Õppematerjalis esines, nii sisu, kui ka ülesehituse suhtes, vigu, mis töö autori poolt hiljem korrigeeriti. Positiivsena toodi välja praktiliste nõuannete olemasolu õppematerjalis.

Välja võib tuua veel selle, et antud töö raames ei töötatud välja erinevaid praktilisi harjutusi mis oleks vaja antud koolituste läbiviimiseks. Järgnevate uurimustööde käigus võiks neid koostada.

Abstract

The aim of this Bachelor's thesis is to create a training material for vocational school students based on the cyber-security specialists' point of view, to increase their knowledge about the dangers of the daily use of the computer and to introduce tools to protect personal information. The study found answers to the following research questions:

1. Which cyber defense knowledge and skills are necessary for vocational school students based on the opinions of cyber-security experts?

2. What should be the structure and content of the training material?

3. How do cyber-security experts evaluate the content and the necessity of training material?

The review of cyber threats and the creation of training materials focuses more on the average user. The work addresses the most common threats from the past, as well as threats that have become more frequent. The theoretical part of the paper gives an overview of the basic knowledge of cyber-security and the basics knowledge of training related literature based on the specialist literature. The data analyze was conducted using a qualitative study method with a thematic content analysis. The sample of the cyber-security expert who evaluated the study material completed in the study consisted of two experts. The created training material could be a tool for vocational school teachers or adults training providers who are intended to educate their trainees about the threats faced by the day-to-day use and protection of the computer and skills to protect personal information.

As a result of the survey, it can be pointed out that there are currently more threats on the Internet and social media that young people should pay attention to when they want to ensure their safety and security. Interviewed experts pointed out that there are gaps in knowledge and skills among young and adults as well. An example of the most common problem was the logging in and out of computers, both for students and teachers. By providing people with knowledge of dangers and guidelines for preventing danger, it is hoped that they will make their everyday activities safer in cyberspace.

Experts found that the training material created is well suited for training vocational school students. In the training material, there were errors in the content, as well as in the structure, which later was corrected by the author. Positive was the introduction of practical advice in the study material.

It should also be pointed out that in the framework of this work, no practical exercises were developed that would be needed to carry out the training. In the course of subsequent research, they should be developed.

Tänusõnad

Tänan küberkaitseeksperte, kes andsid intervjuud ja eksperthinnangud käesoleva uurimustöö koostamiseks. Lisaks soovin tänada küberkaitseeksperti, kes aitas analüüsi käigus kodeerimist parandada ja täiendada. Tänan kõiki, kes andsid nõu töö teoreetilise osa ja õppematerjali koostamisel juures.

Tänan oma töö juhendajat J. Ginter'it, kes toetasid minu lõputöö valmimisel.

Autorsuse kinnitus

Kinnitan, et olen koostanud ise käesoleva lõputöö ning toonud korrektselt välja teiste autorite ja toetajate panuse. Töö on koostatud lähtudes Tartu Ülikooli haridusteaduste instituudi lõputöö nõuetest ning on kooskõlas heade akadeemiliste tavadega.

/Allkiri/

/Kuupäev/

Kasutatud kirjandus

Allas, A., Einasto, H., Kasesalu, A., Mägi, R., Mägi, S., Pahtma, L., Pilliroog, E., Riiberg, K., Saro, A., Süvalep, E., Tamepuu, A., & Tainemaa, S. (2008) Tea laste- ja noorteentsüklopeedia 3. Tallinn: TEA Kirjastus.

Arvutikaitse. (2018) Külastatud aadressil http://www.arvutikaitse.ee/arvutikaitse-algtoed

Atkins, B. & Huang, W. (2013) A study of social engineering in online frauds**.** Open Journal of Social Sciences. Külastatud aadressil http://file.scirp.org/Html/36435.html

Caine, R.N. & Caine, G. (1991) Making Connections: Teaching and the Human Brain. Association for Supervision and Curriculum Development. Külastatud aadressil https://files.eric.ed.gov/fulltext/ED335141.pdf

Ezzy, D. (2002). *Qualitative Analysis: Practice and Innovation*. Crows Nest, NSW: Allen & Unwin.

Giannakas, F., Kambourakis, G., Papasalouros, A. & Gritzalis, S. (2016) Security Education and Awareness for K-6 Going Mobile. Külastatud aadressil http://online-journals.org/index.php/i-jim/article/view/5473/3898

Greitzer, F.L., Strozer, J.R., Cohen S., Moore, A.P. & Mundie, D., Cowley J. (2014) Analysis of unintentional insider threats deriving from social engineering exploits**.** IEEE Security and Privacy Workshops. Külastatud aadressil http://ieeexplore.ieee.org/document/6957309

Hanewald, R. (2008). Confronting the Pedagogical Challenge of Cyber Safety. Australian Journal of Teacher Education, 33(3). Külastatud aadressil http://files.eric.ed.gov/fulltext/EJ1069644.pdf

Haridus– ja Teadusministeerium, Eesti Koostöö Kogu & Eesti Haridusfoorum. (2014) "Eluksetva õppe strateegia 2020" Külastatud aadressil https://www.hm.ee/sites/default/files/strateegia2020.pdf

Hughes, T.F. (2008) Report on Safe Use of the Internet: Some of the Most Common Risks. Vanderbilt Universit. Külastatud aadressil http://www.jstor.org/stable/pdf/20063724.pdf

Kaitseministeerium. „Küberjulgeoleku strateegia 2008–2013." 2008 Külastatud aadressil https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf

Kaitsepolitseiamet. (2016) „Kaitsepolitseiameti aastaraamat 2015“ Külastatud aadressil http://www.digar.ee/arhiiv/nlib-digar:276624

Kansal, Y., Kumar, D. &, Kapur, P. K. (2016) Vulnerability Patch Modeling. Külastatud aadressil http://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=29&sid=24d33913-23d0-4625-a488-1eb6aa87d741%40sessionmgr102

Katsikas, S.K. (2000) Health care management and information systems security: awareness , training or education? International Journal of Medical Informatics. Külastatud aadressil http://www.sciencedirect.com/science/article/pii/S138650560000112X?via%3Dihub

Kirna, A. (2006). Turvaline WiFi. Külastatud aadressil http://www.arvutikaitse.ee/turvaline-wifi/

Kook, K. (2016). Kuidas aru saada, et arvutis on viirus ning mida teha? Külastatud aadressil https://geenius.ee/rubriik/hea-nipp/kuidas-aru-saada-et-arvutis-on-viirus-ning-mida-teha/

Kowalski, R. M., & Limber, S. P. (2007). Electronic Bullying Among Middle School Students. Külastatud aadressil http://www.sciencedirect.com/science/article/pii/S1054139X07003618?via%3Dihub

Krull, E. (2000) Pedagoogilise psühholoogia käsiraamat. TÜ Kirjastus

Kärtner, P., Maiberg, L., Rikker, M., Tuuling, L., Voltein, E. (2006). Õppematerjal koolieelsetelasteasutuste eesti keele kui teise keele õpetajate põhi- ja täienduskoolituseks. Tartu: Kirjastus Atlex.

Laherand, M-L. (2008). Kvalitatiivne uurimisviis. Tallinn: Infotrükk.

Langenderfer, J. & Shimp. T.A. (2001) Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. Psychology & Marketing. Külastatud aadressil http://onlinelibrary.wiley.com/doi/10.1002/mar.1029/epdf

Lorenz, B., Laugasson, E., Püvi, S & Laanpere, M. (2014). DigiTurvis. Külastatud aadressil https://drive.google.com/file/d/0B2oPX5ATEw20YXZkS1ZSQXZ0Zlk/view

Lorenz, B., (2017). A Digital Safety Model for Understanding Teenage Internet User’s Concerns. (Doktoritöö, Tallinn University). Tallinn University: Tallinna Ülikool. Külastatud aadressil: http://www.etera.ee/zoom/30536/view?page=3&p=separate&view=0,0,2067,2834

Luckett, P., McDonald, J. T. & Dawson, J. (2016) Neural Network Analysis of System Call Timing for Rootkit Detection. Külastatud aadressil

http://resolver.ebscohost.com/openurl?sid=EBSCO%3aedseee&genre=book&issn=edseee.IEEEConferenc&ISBN=9781509057719&volume=&issue=&date=&spage=1&pages=1-6&title=2016+Cybersecurity+Symposium+(CYBERSEC)%2c+Cybersecurity+Symposium+(CYBERSEC)%2c+2016%2c+CYBERSEC&atitle=Neural+Network+Analysis+of+System+Call+Timing+for+Rootkit+Detection&aulast=Luckett%2c+Patrick&id=DOI%3a10.1109%2fCYBERSEC.2016.008&site=ftf-live

Majandus- ja Kommunikatsiooniministeerium. (2014) „Küberjulgeoleku strateegia 2014-2017“Külastatud aadressil https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf

McGeehan, J. (2001) Brain-Compatible Learning. Green Teacher vol. 64, 2001, pp. 7-13.
Mikk, J (1993). Mõtlemise arendamine. (Austraalia kogemus) Haridus, 7/8, 19 – 22

Mikk. J. (1995). Mida hinnata õppekirjanduses. Haridus, 2, 27-33.

Mikk, J. (1999) (Toim). Õppekirjandus väärtuste kujundajana. Väärtuskasvatus õppekirjanduses (lk 74-96). Tartu: Tartu Ülikool.

Mikk, J. (2000). Textbook: Research and Writing. Frankfurk am Main; Brerlin; Bruxelles; New York; Oxford; WIEN; Lang, (Baltische Studien zur Erziehungs und Sozialwissenschaft;Bd.3)

Mikk, J. (2001). Textbooks and curriculum. Sixth IARTEM International Conference on Learning and Educational Media. Abstracts, 46 – 47

Mikk, J. (2010). Loengu konspektid aines Pedagoogika Alused. Tartu Ülikool.

Mishna, F., Khoury-Kassabri, M., Gadalla, T., & Daciuk, J. (2012). Risk factors for involvement in cyber bullying: Victims, bullies and bully-victims. Külastatud aadressil http://www.sciencedirect.com/science/article/pii/S0190740911003343?via%3Dihub

Mitnick, K.D. & Simon, W.L. (2006) The art of intrusion. Wiley, Indiana.
Peterson, E. (2003). Oskuslikuks lugejaks – aga kuidas? Teksti- ja lugemisõpetus. Tartu: Atlex.

Politsei ja Piirivalveamet. (2018). Uuenda oma tarkvara esimesel võimalusel. Külastatud aadressil https://www.politsei.ee/et/nouanded/digiturvalisus.dot

Politsei ja Piirivalveamet. (2018). Küberkiusamine. Külastatud aadressil https://www.politsei.ee/et/nouanded/noorele/kuberkiusamine/

Reid, R., Niekerk, J. & Solms, R. (2011) Guidelines for the creation of brain-compatible cyber security educational material in Moodle 2.0. Külastatud aadressil http://icsa.cs.up.ac.za/issa/2011/Proceedings/Full/06_Paper.pdf

Riigi Infosüsteemi Amet, (2008) „Infosüsteemide kolmeastmeline etalonturbe süsteem." Külastatud aadressil https://www.ria.ee/public/ISKE/ISKE_rakendusjuhend_4_01_16122008.pdf

Riigi Infosüsteemi Amet. (2016) „Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. aasta kokkuvõte." Külastatud aadressil https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturbe-aastaraport-2016.pdf

Roosimäe, K (2016). Bioloogia õppematerjali „Mikroorganismid" koostamine ja katsetamine kakskeelse põhikooli 8. klassis. Publitseerimata magistritöö. Tartu Ülikool.

Ruiter, R.A.C., Kessels, L.T.E., Peters, G.Y. & Kok, G. (2014) Sixty years of fear appeal research: Current state of the evidence**.** International Journal of Psychology, 49 (2) Külastatud aadressil http://onlinelibrary.wiley.com/doi/10.1002/ijop.12042/full

Schultz, E. (2004) Security training and awareness—fitting a square peg in a round hole. Computers Security. Külastatud aadressil http://www.sciencedirect.com/science/article/pii/S0167404804000094?via%3Dihub

Sleuers, W. (2001). Educational media policy: Analysis of the problems of small country. IARTEM International Conference on Learning and Educational Media. Abstract. 57

Stemler, S. (2001). An overview of content analysis. Practical Assessment, Research and Evaluation**.** Külastatud aadressil http://pareonline.net/getvn.asp?v=7%26n=17

Zhang, X., Li, C., Peng, W. & Huang, T. (2017) Toward understanding how the human vigilance contains the prevalence of computer viruses. Külastatud aadressil http://resolver.ebscohost.com/openurl?sid=EBSCO:edseee&genre=book&issn=edseee.IEEEConferenc&ISBN=9781509047260&volume=&issue=&date=&spage=12&pages=12-16&title=2017%20Ninth%20International%20Conference%20on%20Advanced%20Computational%20Intelligence%20(ICACI),%20Advanced%20Computational%20Intelligence%20(ICACI),%202017%20Ninth%20International%20Conference%20on&atitle=Toward%20understanding%20how%20the%20human%20vigilance%20contains%20the%20prevalence%20of%20computer%20viruses&aulast=Zhang%2C%20Xianxiu&id=DOI:10.1109/ICACI.2017.7974478

Vabariigi Valitsus. (2016) Kutseharidusstandard. Külastatud aadressil https://www.riigiteataja.ee/akt/116072016008

Valentine, J. (2006) Enhancing the employee security awareness model. Computer Fraud Security. Külastatud aadressil http://www.sciencedirect.com/science/article/pii/S1361372306703700?via%3Dihub

Vetik, L. (2015) Interneti ohutus on iga õpetaja ja kooli väljakutse. Külastatud aadressil https://koolielu.ee/info/readnews/467714/internetiohutus-on-iga-opetaja-ja-kooli-valjakutse

Viiruste ja muu ründevara tõkestamine ja eemaldamine. (2017) Külastatud aadressil https://support.microsoft.com/et-ee/help/129972/how-to-prevent-and-remove-viruses-and-other-malware

Williams, E., Beardmore, A., & Joinson, A. (2017) Individual differences in susceptibility to online influence: A theoretical review Külastatud aadressil http://www.sciencedirect.com/science/article/pii/S0747563217301504?via%3Dihub

Lisad

Lisa 1

Intervjuu küsimustik

Uurimustöö eesmärk

Lähtuvalt küberkaitseekspertide arvamusest koostada kutsekoolidele küberkaitsealase algteadmiste õppematerjal.

Intervjuu läbi viimine

Intervjuu viiakse läbi kolme Eesti küberkaitseeksperdiga. Tegemist on personaalintervjuudega, seepärast lepitakse intervjueeritavatega aegsasti kokku sobiv kohtumisaeg. Intervjueerimise kohana kasutatakse võimalusel privaatset ruumi, kus intervjuu läbiviimise ajal ei oleks kõrvalisi isikuid. Intervjuu kestust on planeeritud orienteeruvalt üks tund. Autor saadab küsimused enne intervjuu toimumist vastajale, et ta saaks teema läbi mõelda. Küsimuste varasem saatmine annab ekspertidele võimaluse põhjendatud ja läbimõeldud arvamust avaldada.

Tabel 1. Ekspertide andmed. Ekspertide tähistust E tähistab küberkaitseeksperti.

Ekspert	Praegune amet	Haridus	Tööstaaž küberkaitse valdkonnas
E1	Õpetaja	TTÜ Küberkaitse magister	4,5 aastat
E2	Spetsialist	TTÜ Küberkaitse magister	4 aastat
E3	Spetsialist	TTÜ Küberkaitse magister	6 aastat

Intervjuu küsimused:

1. Milline on Teie haridus küberkaitse valdkonnas?
2. Milline on Teie kogemus küberkaitse valdkonnas töötamisel või uurimisel?
3. Millised on Teie kogemused kutsekooliõpilaste ja lõpetanute tegevusest arvutitega ja internetis?
4. Milliseid küberkaitse meetmetega seotud teadmisi ja oskusi vajavad noored, kes kasutavad arvuteid ja internetti?

5. Millised küberkaitse meetmetega seotud teadmised ja oskused on tänapäeva noortel puudu?
6. Millised ohud tulenevad puudulikest teadmistest ja oskustest?
7. Loetlege valdkonnad või teemad, mida tuleks Teie arvates kindlasti kutsekoolis õpetada.
8. Milline peab Teie arvates olema õppematerjali sisu?
9. Milline peab Teie arvates olema õppematerjali ülesehitus?

Lisa 2

Tagasiside ankeet

Lugupeetud vastaja!

Olen Tartu Ülikooli sotsiaal- ja haridusteaduskonna bakalaureuseõppe kutseõpetaja eriala tudeng Madli Valtenberg. Bakalaureusetöö teemaks on õppematerjali koostamine. Töös käsitlen küberkaitsealaseid algteadmisi kutsekooli õpilastele ja õppematerjal on koostatud kasutamiseks kutseõppes või täiskasvanute koolitustel. Palun tutvuge koostatud õppematerjaliga ja andke sellele tagasiside, vastates ankeedis toodud küsimustele. Teie poolt antud tagasiside ning ettepanekute põhjal teen muudatused õppematerjalis.

Lisa info saamiseks on alljärgnevad kontaktid:

Telefon:

E-mail:

Ette tänades

Madli Valtenberg

1. Milline on Teie haridus küberkaitse valdkonnas?
2. Milline on Teie kogemus küberkaitse valdkonnas töötamisel või uurimisel?

Järgnevate väidete korral valige, palun, kõige täpsemini sobiv vastusevariant.

1 Täiesti nõus 2 Pigem nõus 3 Nii ja naa 4 Pigem ei ole nõus 5 Ei nõustu üldse

3. Õppematerjal on kutseõpilastele jõukohane.
4. Õppematerjali osad on omavahel hästi seotud.
5. Õppematerjal on hästi loetav.
6. Õppematerjal on selge struktuuriga.

7. Õppematerjali laused on arusaadavad
8. Õppematerjali sisu on otstarbekalt selgitatud.
9. Õppematerjali sisu annab antud teemast ülevaate.
10. Õpitavate teemade tähtsust on hästi näidatud.
11. Õppematerjal võimaldab saavutada õpieesmärgid.
12. Mis on Teie arvates õppematerjali juures positiivset?

.....

.....

.....

.....

.....

.....

13. Mis on Teie arvates õppematerjali juures negatiivset?

.....

.....

.....

.....

.....

.....

14. Mida võiks Teie arvates õppematerjalis juures muuta?

.....

.....

.....

.....

.....

.....

15. Kui Teil on täiendavaid tähelepanekuid õppematerjali osas, siis palun kirjutage.

.....

.....

TÄNAN!

Õppematerjal “Küberkaitse algteadmised”.

ÜLESEHITUS

- Sissejuhatus
- Eesmärk
- Enamlevinud ohud (kirjeldus, päritolu, kuidas äratunda, vältida ja eemaldada)
- Üldised nõuanded
- Soovituslik vaatamine
- Küsimused
- Kasutatud kirjandus

EESMÄRK

Antud koolituse eesmärk on tõsta küberkaitsealaseid teadmisi igapäevase arvuti ja sotsiaalmeedia kasutamisel ning tutvustada abivahendeid isiklike seadmete ja info kaitsmiseks.

ENAMLEVINUD OHUD

1. Pahavara (arvutiviirused, ussviirused, Trooja Hobune, nuhkvara, petturlik turvatarkvara, reklaamvara ja lunavara)
2. Juurkomplekt e. Rootkit
3. Tarkvara turvaaugud
4. *Social engineering*

PAHAVARA

(arvutiviirused, ussviirused, Trooja Hobune, nuhkvara petturlik turvatarkvara ja reklaamvara)

MIS ASI ON PAHAVARA?

Arvutisüsteemi kahjustamiseks või soovimatute toimingute tegemiseks loodud pahatahtlik tarkvara, mida nimetatakse pahavaraks.

ARVUTIVIIRUSED

“Arvutiviirus on sõltumatu alamprogramm, mis ennast taastootes teostab süsteemides, teistes programmides või nendega seotud keskkondades manipulatsioone, mis ei ole kasutaja poolt kontrollitavad” (Riigi Infosüsteemi Amet, 2008, lk 22)

USSVIIRUSED

Ussviirus on programmkood mis tavaliselt levib kasutaja sekkumiseta. Ta levib meilisõnumite, võrkude või operatsioonisüsteemi turvaaukude kaudu automaatselt.

TROOJA HOBUNE

Troojalane ehk „Trooja hobune“ on teistesse programmidesse peidetud pahavara.

NUHKVARA

Nuhkvara on programm, mis kogub kasutaja arvutist informatsiooni ning saadab selle edasi infost huvitatud osapoolele.

REKLAAMVARA

Reklaamvara on tarkvara, mis laetakse kasutaja arvutisse, mis esitab või kuvab automaatselt reklaame.

LUNAVARA

Lunavara (ransomware) on selline pahavaramis krüptib kasutaja arvutis kas olulised andmed või terve kõvaketta. Seejärel nõuavad kurjategijad andmete lahtikrüptimisvõtme eest lunaraha.

KUIDAS ARU SAADA, ET ARVUTIS ON PAHAVARA?

1. Seadme töö on häiritud.
2. Ei tööta nii nagu tavaliselt.
3. Seade ei tööta enam.
4. Seade on aeglane või “jookseb” kokku.
5. Popup teated või reklaamid.
6. Hüpikreklaamid.

KUIDAS ENNETADA?

1. Tulemüür.
2. Viirusetõrje.
3. Nuhkvara tõrje programmi.
4. Ära ava manuseid ja linke, mille usaldusväärsuses kindel ei ole.
5. Üra lae alla ebausaldusväärseid programme ebausaldusväärsetest allikatest.
6. Ole ettevaatlik failijagamise veebilehtede puhul
7. Ära vajuta suvaliste hüpikakende linkidele
8. Jälgi, et süsteem ja tarkvara on uuendatud.

KUIDAS NEID EEMALDADA?

1. Kasuta viirusetõrje programmi.
2. Kasuta spetsiaalset nuhkvara tõrje programmi.
3. Lunavara eemaldamise tarkvara.
4. Reklaamvara eemaldamise tööriistad.
5. Spetsialisti abiga.

JUURKOMPLEKT EHK *ROOTKIT*

Termin rootkit viitab programmile, millel on arvutis juurõigused ja millel on kaasas tööriistad, millega arvutit manipuleerida. Juurõigused tähendab, et programmil on juurdepääs administraatori kontole süsteemis ja see annab programmile võimaluse failide muutmiseks.

KUIDAS SEDA ÄRA TUNDA, ENNETADA JA EEMALDADA?

1. Tuvatamine on keeruline.
2. Viirustõrje programmid.
3. Eemaldatakse käsitsi (professionaalse spetsialisti töö).

TARKVARA TURVAAUGUD

Turvaauk on arvutiprogrammi või -süsteemi loomise käigus tekkinud viga, kas ei mõeldud korralikult läbi või ei osatud ette näha, loodi hooletult või otsustati ignoreerida ning mille kaudu saab seda kuritarvitada.

KUIDAS ÄRA TUNDA, ENNETADA JA EEMALDADA?

- Keeruline tuvastada.
- Automaatne uuenduste paigaldamine.
- Turvapalaastri ja teiste programmiparanduste alla laadimine ja paigaldamine
- Tarkvara oleks õigeaegselt paigatud ja uuendatud.
- Süsteemi uuendamine

SOCIAL ENGINEERING

Püüdlus ebaseaduslikku kasu saamise eesmärgil inimesi psühholoogiliselt mõjutada ja nendega manipuleerida kasutades sotsiaalvõrgustikke või siis IKT vahendeid ja teenuseid.

KUIDAS SEE KÄIB?

Internetipetturid loovad stsenaariume, kasutades sageli paanikat, põnevust, uudishimu või empaatiat puudutavaid emotsionaalseid käivitavaid tegureid, et julgustada inimesi vigu tegema oma otsuste langetamisel.

KUIDAS SEDA ÄRA TUNDA?

- Tavaliselt üksikisiku manipuleerimine.
- Julgustamisele ohtlike toimingute tegemiseks.

KUIDAS VÄLTIDA?

1. Ära ava võõraid e-kirju.
2. Ära avalikusta oma isikliku teavet võõrastele.
3. Ära võta vastu kingitusi (USB seadmed jms) võõrastelt.
4. Veendu, et isikud kellega suhtled on isikud, keda sa usud olevat.

KUIDAS ENNETADA?

1. Kaitse oma privaatsust.
2. Kasuta viirusetõrje programme.
3. Kasuta tugevaid paroole.
4. Kasuta kaheastmelist autentimist.
5. Kasuta usaldusväärset tarkvara, seadmeid ja internetiühendusi.

ÜLDISED NÕUANDED

TURVALINE VEEBILEHITSEMINE

1. Teadlikkus erinevatest veebilehitsejatest läbi turvalisuse vaatepunkti.
2. Turvaliste lisandite kasutamine veebilehitsejates.
3. Turvalise ühenduse (https) kasutamine;
4. Veebilehe identiteedi jälgimine.
5. Privaatse režiimi käivitamine ja selle vaikimisi määramine.
6. Kogemata veebilehitsejale meeldejäetud kasutajate, salasõnade kustutamine.

OLUKORRATEADLIKUS

1. Teadlikkus nuhkimise, jälitamise võimalikkusest ja kuidas seda vältida ning mida teha kui on juhtunud intsident.
2. Teadlikkus sotsiaalse manipuleerimise eri tahkudest ja kuidas neid vältida ning mida teha kui on juhtunud intsident.
3. Prügi sorteerimine (süsteemi jääkandmed ja paber materjalide hävitamine).
4. Kaitse oma andmeid sotsiaalmeedias (Facebookis jne)

"Kahtlasest aadressist või õngitsuskirjast anna teada e-posti aadressil cert@ cert.ee " (Riigi Infosüsteemi Ameti, 2016, lk 13)

TURVALINE SALASÕNA

- Enne parooli ja kasutajanime sisestamist veendu, et tegemist on tegeliku teenusepakkuja veebilehega.
- Väldi paroolide ristkasutamist.
- *"Lülita võimalusel sisse kaheastmeline autentimine, eriti e-posti kontol. Juhendid selleks leiad RIA blogist (blog. ria.ee)."* (Riigi Infosüsteemi Ameti, 2016, lk 13)

VARUNDAMINE

- Failide varundamise tähtsusest ning turvalisusest ja ristkasutuse võimalustest eri seadmete ja kasutajate vahel.
- Pilvepõhiste salvestusvõimaluste valik, sh turvalisuse vaatepunktist.
- Andmete ja kontaktide varundamine.

ARVUTI PUHASTAMINE

1. Rämpsposti ei ole mõtet koguda.
2. *"Ära ava manuseid ja linke, mille usaldusväärsuses sa kindel ei ole.*(...) *Kahtlane e-kiri edasta koos päiste ja manusega aadressile cert@cert.ee (või laadi üles https://paste.cert.ee) ning kustuta kiri ise kohe."* (Riigi Infosüsteemi Ameti, 2016, lk 10)

MINU DIGITAALNE JALAJÄLG

Mis see on?

SOOVITUSLIK VAATAMINE

1. Targalt Internetis veebileht http://www.targaltinternetis.ee/
2. Arvutikaitse http://www.arvutikaitse.ee
3. Nutiturvalisus http://www.nutiturvalisus.ee/
4. Nutiseadme turvaline kasutus http://www.pariseltkavoi.ee/
5. Interneti käitumine http://noor.targaltinternetis.ee/
6. Arvuti turve http://ekaitse.ee
7. Tasuta viirusetõrje https://www.avast.com

Küsimusi?

KASUTATUD KIRJANDUS

- Allas, A., Einasto, H., Kasesalu, A., Mägi, R., Mägi, S., Pahtma, L., Pilliroog, E., Riiberg, K., Saro, A., Süvalep, E., Tamepuu, A., & Tainemaa, S. (2008) Tea laste- ja noorteentsüklopeedia 3. Tallinn: TEA Kirjastus.
- Arvutikaitse. Külastatud aadressil http://www.arvutikaitse.ee/arvutikaitse-alatoed
- Atkins, B. & Huang, W. (2013) A study of social engineering in online frauds. Open Journal of Social Sciences. Külastatud aadressil http://file.scirp.org/Html/3b435.html
- Caine, R.N. & Caine, G. (1991) Making Connections: Teaching and the Human Brain. Association for Supervision and Curriculum Development. Külastatud aadressil https://files.eric.ed.gov/fulltext/ED335141.pdf
- Eesti keele seletav sõnaraamat. Külastatud aadressil http://www.eki.ee/dict/ekss/index.cgi?Q=k%C3%BCberruum&F=M
- Ezzy, D. (2002). *Qualitative Analysis: Practice and Innovation*. Crows Nest, NSW: Allen & Unwin.
- Fleming, N., & Baume, D. (2006). Learning Styles Again: VARKing up the right tree! Educational Developments, 7(4), 4–7.

KASUTATUD KIRJANDUS

- Greitzer, F.L., Strozer, J.R., Cohen S., Moore, A.P. & Mundie, D., Cowley J. (2014) Analysis of unintentional insider threats deriving from social engineering exploits. IEEE Security and Privacy Workshops. Külastatud aadressil http://ieeexplore.ieee.org/document/6957309/
- Hanewald, R. (2008). Confronting the Pedagogical Challenge of Cyber Safety. Australian Journal of Teacher Education, 33(3). Külastatud aadressil http://files.eric.ed.gov/fulltext/EJ1069644.pdf
- Hughes, T.F. (2008) Report on Safe Use of the Internet: Some of the Most Common Risks. Vanderbilt Universit. Külastatud aadressil http://www.jstor.org/stable/pdf/20063724.pdf
- Kaitseministeerium. „Küberjulgeoleku strateegia 2008–2013." 2008 Külastatud aadressil https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf
- Kaitsepolitseiamet. (2016) „Kaitsepolitseiameti aastaraamat 2015" Külastatud aadressil http://www.digar.ee/arhiiv/nlib-digar:276624
- Kansal, Y., Kumar, D. &, Kapur, P. K. (2016) Vulnerability Patch Modeling. Külastatud aadressil http://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=29&sid=24d33913-23d0-4625-a488-1e6baa87d741%40sessionmgr102
- Kirna, A. (2006). Turvaline WiFi. Külastatud aadressil **http://www.arvutikaitse.ee/turvaline-wifi/**
- Kook, K. (2016). Kuidas aru saada, et arvutis on viirus ning mida teha? Külastatud aadressil https://geenius.ee/rubriik/hea-nipp/kuidas-aru-saada-et-arvutis-on-viirus-ning-mida-teha/

KASUTATUD KIRJANDUS

- Kowalski, R. M., & Limber, S. P. (2007). Electronic Bullying Among Middle School Students. Külastatud aadressil http://www.sciencedirect.com/science/article/pii/S1054139X07003618?via%3Dihub
- Langenderfer, J. & Shimp. T.A. (2001) Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. Psychology & Marketing. Külastatud aadressil http://onlinelibrary.wiley.com/doi/10.1002/mar.1029/epdf
- Lorenz, B., Laugasson, E., Püvi, S & Laanpere, M. (2014). DigiTurvis. Külastatud aadressil https://drive.google.com/file/d/0B2oPXSATEw20YXZkS17SQlX2QTk/view
- Luckett, P., McDonald, J. T. & Dawson, J. (2016) Neural Network Analysis of System Call Timing for Rootkit Detection. Külastatud aadressil http://resolver.ebscohost.com/openurl?sid=EBSCO%3aedseee&genre=book&issn=edseee.IEEECoperenc&isbN=9781509057719&volume=&issue=&date=&spage=1&pages=1-8&title=2016+Cybersecurity+Symposium+(CYBERSEC)%2C+Cybersecurity+Symposium+(CYBERSEC)%2c+2016%2c+CYBERSEC&atitle=Neural+Network+Analysis+of+System+Call+Timing+for+Rootkit+Detection&aulast=Luckett%2C+Patrick&id=DOI%3a10.1109%2fCYBERSEC.2016.008&site=ftf-live
- Majandus- ja Kommunikatsooniministeerium. (2014) „Küberjulgeoleku strateegia 2014-2017"Külastatud aadressil https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf

KASUTATUD KIRJANDUS

- Mishna, F., Khoury-Kassabri, M., Gadalla, T., & Daciuk, J. (2012). Risk factors for involvement in cyber bullying: Victims, bullies and bully-victims. Külastatud aadressil http://www.sciencedirect.com/science/article/pii/S0190740911003343?via%3Dihub
- Mitnick, K.D. & Simon, W.L. (2006) The art of intrusion. Wiley, Indiana.
- Politsei ja Piirivalveamet. (2018). Küberkiusamine. Külastatud aadressil https://www.politsei.ee/et/nouanded/noorele/kuberkiusamine/
- Reid, R., Niekerk, J. & Solms, R. (2011) Guidelines for the creation of brain-compatible cyber security educational material in Moodle 2.0. Külastatud aadressil http://icsa.cs.up.ac.za/issa/2011/Proceedings/Full/06_Paper.pdf

KASUTATUD KIRJANDUS

- Riigi Infosüsteemi Amet, (2008) „Infosüsteemide kolmeastmeline etalonturbe süsteem." Külastatud aadressil https://www.ria.ee/public/ISKE/ISKE_rakendusjuhend_4_01_16122008.pdf
- Riigi Infosüsteemi Amet. (2016) „Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. aasta kokkuvõte." Külastatud aadressil https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturbe-aastaraport-2016.pdf
- Riigiportaali kodulehekülg. E-teenused. Külastatud aadressil https://www.eesti.ee/est/teenused
- Ruiter, R.A.C., Kessels, L.T.E., Peters, G.Y. & Kok, G. (2014) Sixty years of fear appeal research: Current state of the evidence. International Journal of Psychology, 49 (2) Külastatud aadressil http://onlinelibrary.wiley.com/doi/10.1002/ijop.12042/full
- Schultz, E. (2004) Security training and awareness—fitting a square peg in a round hole. Computers Security. Külastatud aadressil http://www.sciencedirect.com/science/article/pii/S0167404804000094?via%3Dihub
- Siseministeerium. (2016) „Turvalisuspoliitika 2008-2015: kokkuvõte "Turvalisuspoliitika põhisuunad aastani 2015" täitmisest." lk 24-26,Külastatud aadressil https://issuu.com/siseministeerium/docs/turvalisuspoliitika_kokkuvote
- Targalt internetis. Küberkiusamine. Külastatud aadressil http://noor.targaltinternetis.ee/kuber-kiusamine/

KASUTATUD KIRJANDUS

- Zhang, X., Li, C., Peng, W. & Huang, T. (2017) Toward understanding how the human vigilance contains the prevalence of computer viruses. Külastatud aadressil http://revolver.ebscohost.com/openurl?sid=EBSCO:edsieee&genre=book&issn=ediseee.IEEEConferenc&ISBN=9781509047260&volume=&issue=&date=&spage=12&pages=12-16&title=2017%20Ninth%20International%20Conference%20on%20Advanced%20Computational%20Intelligence%20(ICACI)%20Advanced%20Computational%20Intelligence%20(ICACI),%202017%20Ninth%20International%20Conference%20on&atitle=Toward%20understanding%20how%20the%20human%20vigilance%20contains%20the%20prevalence%20of%20computer%20viruses&aulast=Zhang%2C%20Xianxiu&id=DOI:10.1109/ICACI.2017.7974478
- Valtenberg, U. (2012). Eesti Kaitseväe Küberkaitse Treening- ja Harjutuskeskkonna (KTHK)kasutamise võimalused, lähtudes KTHK võimekusest tõna ja tulevikus. Publitseerimata magistritöö. Tallinna Tehnikaülikool.
- Vetik, I. (2016) Milleks gümnasistile küberkaitse? Külastatud aadressil https://koolielu.ee/uudiskiri/readnews/570039/milleks-gumnasistile-kuberkaitse
- Viiruste ja muu rünnavara tõkestamine ja eemaldamine. Külastatud aadressil https://support.microsoft.com/et-ee/help/129972/how-to-prevent-and-remove-viruses-and-other-malware
- Williams, E., Beardmore, A., & Joinson, A. (2017) Individual differences in susceptibility to online influence: A theoretical review Külastatud aadressil http://www.sciencedirect.com/science/article/pii/S0747563217301504?via%3Dihub

Lisa 4

Juhend õppematerjali “Küberkaitse algteadmised” koolitajale.

Antud õppematerjali koostamisel on lähtutud Madli Valtenbergi bakalaureuse töö “Küberkaitsealaste algteadmiste õppematerjali koostamine kutsekooli õpilastele” teooriaosast ja empiirilisest uuringust. Antud õppematerjali autor on seisukohal, et õppematerjal annab õppijale algteadmised küberkaitsevaldkonnast ja on õpetajal lihtsalt kasutatav. Võimalikeks probleemideks ja piiranguteks antud õppematerjali kasutamisel võivad olla keeleoskus ja koolitusel osalejate vähene tehniline kogemus, mille tõttu tuleb räägitavat selgitada. Lisamaterjali avamine vajab interneti ühendust.

Kellele?

Antud õppematerjal on kasutamiseks kutsekooli õpilaste või täiskasvanute täienduskoolitustel, küberkaitsealaste algteadmiste andmiseks.

Koolituse sisu.

Õppematerjalis tutvustatakse levinuimaid ohte ja vastumeetmeid nendele. Õppematerjalis ei käsitleta nutiseadmeid ja keskendutakse ohtudele läbi arvuti vaatevinkli. Koolitusel kasutatavad ülesanded on vaja eelnevalt ette valmistada, võimalusel arvestades koolitatavate teadmiste ja tasemega.

Metoodika.

Õpetamisel tuleb kasutada “aju ühilduva õppimise“ põhimõtteid, näidates koolitatavatele, et nad puutuvad küberohtudega igapäevaselt kokku ja antud valdkond on neile isiklikult tähtis. Videotega tuleb tekitada emotsioone, sest kõik mida koolitatavad õpivad, on mõjutatud emotsioonide ja mõttelaadi poolt.

Kuidas õppematerjali kasutada.

Enne koolitust:

Kuna antud valdkond on kiiresti arenev, siis tuleb ettevalmistuste käigus õppematerjali sisu kaasajastada.

Lisaks tuleb enne koolitust ette valmistada praktilised harjutused ja leida nende läbiviimiseks

vajalikud vahendid.
Soovituslikult tuleks koostada ka teadmiste kontrolli test, mida sooritatakse enne ja pärast koolitust. See annab koolitajale informatsiooni koolitatavate tasemest ja koolitatavad saavad näha oma edasiarengut.

Koolitus.
Slaididel on kokkuvõtlik informatsioon ja kommentaarides on lisa informatsioon, mida peab tegema kas siis selgita, näita või tee harjutus. Lisaks sisaldab see informatsiooni, mida tuleb slaidi juurde rääkida.
NÄITEKS SLAID 1 kommentaarid:
Koolitusel osalejate tervitamine ja enesetutvustus.
Selgita, et esilehe pilt on pärit https://venomit.com/cyber-security-solutions/ veebilehelt.
Selgita:
•et antud õppematerjal on kasutamiseks kutsekooli õpilaste või täiskasvanu õppes küberkaitsealaste algteadmiste andmiseks.
•et õppematerjalis tutvustatakse levinuimaid ohte ja vastumeetmeid nendele.
•et antud õppematerjalis ei käsitleta nutiseadmei ja keskendutakse ohtudele läbi arvuti vaatevinkli.
•et õppematerjalis kasutatud pildid on pärit https://www.avast.com veebilehelt.

Abimaterjalid.
SLAID 2
Lisaks näidata etteantud videot meeleolu loomiseks, näidates läbi huumori, millised ohud tavainimesi ohustavad. Võimalusel vaadata videot alates 1.6 min.

SLAID 15
Peale materjali esitamist tuleb teha koos koolitatavatega järgmised ülesanded:

1. Kasutaja loomine ja õiguste andmine.
2. Reklaamide blokeerimine.
3. Tarkvara peale ja maha installeerimine.

SLAID 27
Näita alustuseks etteantud videot, et näidata, kui lihtne on võimalik kätte saada andmeid millega saab ligi sinu isiklikele asjadele.

SLAID 29

Peale slaid tehke koolitatavatega veebilehitseja turvaseadete seadistamise ülesanne.

SLAID 30

Enne materjali esitamist näidake etteantud videot, mis näitab, kuidas me ise anname oma andmeid välja interneti vahendusel.

Peale materjali esitamist tehke andmete tegeliku kustutamise ülesanne.

SLAID 31

Enne materjali esitamist näidake etteantud videot, et näidata, kui lihtsalt inimesed, läbi väikese manipulatsiooni, ise oma andmeid avaldavad.

Peale materjali esitamist tehke turvalise salasõna loomise ülesanne ja kontrollige selle tugevust.

SLAID 32

Tehke andmete varundamine praktilise ülesandena läbi.

SLAID 33

Tehke praktilise ülesandena e-kirja postkasti puhastamine.

SLAID 34

Laske koolitavatel otsida internetist enda kohta informatsiooni.

SLAID 35

Selgitage, et enese harimine on oma turvalisuse tagamise juures oluline.

Peale koolitust.

Paranda ja täienda õppematerjali vastavalt sellele kas koolituse käigus tekkis tähelepanekuid, näiteks millele rohkem tähelepanu võiks pöörata jne.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Madli Valtenberg (21.09.1977),

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Küberkaitsealaste algteadmiste õppematerjali koostamine kutsekooli õpilastele.", mille juhendaja on Jüri Ginter,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, 10.01.2018