VALIKÕPPEAINE / VALIKKURSUS "KÜBERKAITSE"

AINEKAVA

Tallinn 2017

Sisukord

1 Valikõppeaine "Küberkaitse"

Valikõppeaine „Küberkaitse“ eesmärgiks on anda õpilastele ettekujutus küberkaitse olemusest ja distsipliinidest ning võimaldada neil omandada algteadmised antud valdkonnas.

Ainekavas sisalduva õppetegevuse kaudu omandatakse küberkaitse valdkonna üldised teadmised, mis kinnistatakse praktilise tegevuse kaudu. Õppeaine eesmärk on panna alus turvalise küberkeskkonna põhimõtete mõistmisele, kujundada õpilaste turvateadlikkust ja valmisolekut vajadusel toetada kogukondliku küberturvalisuse teadlikkuse tõstmist.

Ainekava loomisel on võetud aluseks Põltsamaa Ühisgümnaasiumis süvendatult õpetatava valikaine "Küberkaitse" ainekava ning selle senise õpetamise praktilised kogemused, samuti teistes Eesti koolides seni õpetatud küberkaitse temaatikat käsitlevate õppeainete ainekavad ning nende õpetamise praktilised kogemused.

Ainekava põhineb muuhulgas järgmistel dokumentidel, mudelitel, strateegiatel, standarditel, jms:

- Õppijate digipädevusmudel: HITSA, 2016. [http://innovatsioonikeskus.ee/sites/default/files/Digipadevused/Digipadevusmudel_2016.pdf]
- Rahvusvaheline digipädevuse raamistik DIGCOMP 1.0: Euroopa Komisjon, Teadusuuringute Ühiskeskus, Tulevikutehnoloogiate Instituut, 2013. [https://www.hm.ee/sites/default/files/digipadevuse_enesehindamise_raamistik_0.pdf]
- Rahvusvaheline digipädevuse raamistik DIGCOMP 2.0: Euroopa Komisjon, Teadusuuringute Ühiskeskus, 2016. [http://publications.jrc.ec.europa.eu/repository/bitstream/JRC101254/jrc101254_digcomp%202.0%20the%20digital%20competence%20framework%20for%20citizens.%20update%20phase%201.pdf]
- Rahvusvaheline digipädevuse raamistik DIGCOMP 2.1: Euroopa Komisjon, Teadusuuringute Ühiskeskus, 2017. [http://publications.jrc.ec.europa.eu/repository/bitstream/JRC106281/web-digcomp2.1pdf_%28online%29.pdf]
- Gümnaasiumi riiklik õppekava: Kinnitatud VVM Nr 2, 06.01.2011 (RT I, 14.01.2011, 2). Muudetud 15.09.2011 (RT I, 20.09.2011, 1), 02.05.2013 (RT I, 07.05.2013, 10), 22.08.2013 (RT I, 28.08.2013, 1), 20.03.2014 (RT I, 25.03.2014, 7), 28.08.2014 (RT I, 29.08.2014, 18). [https://www.riigiteataja.ee/akt/129082014021]
- Informaatika valikaine IKT riiklik õppekava informaatikaõpetuses: Kinnitatud VVM Nr 1, 06.01.2011 (RT I, 14.01.2011, 1), lisa 10. [https://www.riigiteataja.ee/aktilisa/1290/8201/4020/1m%20lisa10.pdf]
- Küberjulgeoleku strateegia 2014-2017: Majandus- ja Kommunikatsiooniministeerium, 2014. [https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf]
- Elukestva õppe strateegia: Haridus- ja Teadusministeerium, 2014. Kinnitatud VVK 13.02.2014 (RT III, 19.02.2014, 3) [https://www.hm.ee/et/elukestva-oppe-strateegia-2020]

- Digipöörde programm: Haridus- ja Teadusministeerium, 2014 [https://htm.ee/et/tegevused/digipoore-0] [https://www.hm.ee/sites/default/files/2_digipoorde_programmi_2017-2020_eelnou_1.pdf]
- 21. sajandil õppimine/ Partnership for 21st Century Learning: P21, Washington, DC, 2015. [http://www.p21.org/our-work/p21-framework]
- Rahvusvahelise Haridustehnoloogia Seltsi digipädevuste standard: International Society for Technology in Education (ISTE), 2017. [https://www.iste.org/]
- Arvutioskuste sertifitseerimisprogramm European Computer Driving License (ECDL): ECDL Foundation, 1997 – 2017. [http://ecdl.org/]
- Kutsekoda (IKT valdkonna ametid): SA Kutsekoda, 2017. http://www.kutsekoda.ee/]
- IT erialad StartIT: Infotehnoloogia ja Telekommunikatsiooni Liit, 2017. [http://startit.ee/]
- Rajaleidja erialade valikud ja testid: SA Innove, 2017. [http://www.rajaleidja.ee/noor]

Ainekava on koostanud Eesti NATO Ühingu egiidi all tegutsenud töörühm, mille koosseisu kuulusid:

- Birgy Lorenz (Pelgulinna Gümnaasiumi IT-arendusjuht, Eesti Informaatikaõpetajate Seltsi juhatuse liige) - ekspert
- Triin Muulmann (Kehtna Kutsehariduskeskuse informaatikaõpetaja) - ekspert
- Rain Ottis (Tallinna Tehnikaülikooli Tarkvarateaduse instituudi dotsent) - ekspert
- Rein Põdra (Kommunikatsiooni ja Infoturbe Uurimis- ja Arenduskeskus OÜ juhatuse liige) - ekspert
- Tiia Sõmer (Tallinna Tehnikaülikooli Tarkvarateaduse instituudi doktorant-nooremteadur) - ekspert
- Anto Veldre (Riigi Infosüsteemi Ameti analüütik) - ekspert
- Tiia Mikson (Põltsamaa Ühisgümnaasiumi õppealajuhataja) - kolleegiumi liige
- Krista Mulenok (Eesti NATO Ühingu juhatuse liige) - kolleegiumi liige
- Hindrek Lootus (vabakutseline konsultant ja koolitaja) - töörühma juht

Ainekava valmimisele aitasid oma nõuannete ja soovitustega kaasa Haridus- ja Teadusministeeriumi IT-nõunik Jaak Anton, sama ministeeriumi peaekspert Signe Granström ning mitmed Põltsamaa Ühisgümnaasiumi, Tartu Jaan Poska Gümnaasiumi, Tartu Tamme Gümnaasiumi, Jõhvi Gümnaasiumi, Elva Gümnaasiumi ning Rocca al Mare Kooli õpetajad ja töötajad, kellele kõigile töörühm avaldab selle eest siirast ja sügavat tänu. Ainekava tugevad küljed on nõustajate teene, kõigi võimalike puudujääkide eest vastutab üksnes töörühm.

2 Õppeaine kirjeldus

Valikaine 'Küberkaitse' on küberkaitse teemaliste kursuste kogumik.

Esimene baaskursus, **INFOÜHISKOND JA ISIKLIK TURVALISUS**, ei eelda erialateadmisi küberkaitsest, kuid eeldab, et informaatika ja ühiskonnaõpetuse baasalused, õppijate digipädevusmudeli III aste on põhikoolis omandatud ning et õpilastel on olemas valdkonna keerukuse mõistmiseks vajalikud pädevused digitaalses ohutuses ja küberhügieenis. Huvitatud koolidel on võimalus baaskursus aluseks võtta või luua selle põhjal oma kooli ainekava ja töökava.

Soovitame kursuse vältel korraldada erinevaid õppekäike ja kutsuda väliskülalisi: kaasata inimesi Kaitseliidu Küberkaitse üksusest (KL KKÜ), kohaliku omavalitsuse esindajaid, infoturbespetsialiste ja juriste nii avalikust kui ka erasektorist ja ülikoolidest. See tõstab antava kursuse väärtust.

Küberhügieen on käesoleva õppeaine kontekstis defineeritud kui kasutaja poolt asjakohaste turbemeetmete kasutusele võtmine IT süsteemide ja seadmete kasutamisel ning küberturvalisuse parimate praktikate järgimine.

Edasised kooli poolt loodavad valikkursused võimaldavad koolil õpilastel arendada oma huvist ja võimalustest tulenevaid kompetentse, nt. läbi järgmiste kursuste:

- tehnilised küberkompetentsid (kaitse ja rünne);
- võrguturve ja haldus;
- droonid ja robootika küberkaitse teenistuses;
- riik, meditsiin ja küberkaitse jne.

3 Õppeainete lõiming teiste ainevaldkondadega

INFOÜHISKOND JA ISIKLIK TURVALISUS on multidistsiplinaarne kursus, millel on tihedaid kokkupuutepunkte mitmete teiste gümnaasiumi õppekava õppeainetega:

- ühiskonnaõpetus – kodanikukasvatus, riigikaitse korraldus, kaitseväe ja Kaitseliidu struktuur, Euroopa Liit, NATO ja ÜRO, rahvusvahelised kriisid ja konfliktid, Eesti kaitsepoliitika;
- üldajalugu – sõjaajalugu, kriiside ja konfliktide tekkepõhjused ning tagajärjed, rahvusvahelised kriisid ja konfliktid, Euroopa Liit, NATO ja ÜRO;
- riigikaitseõpetus – militaarstruktuurid, riigikaitse ülesehitus;
- eesti keel – terminoloogia, töö juriidiliste tekstidega, suuline ja kirjalik eneseväljendusoskus;
- võõrkeeled – terminoloogia;
- karjääriõpetus - karjääri ja edasise õppimise planeerimine;

- majandus- ja ettevõtlusõpe - ühiskonna toimemehhanismid, majanduse edukuse ja kahju seos digitaalse valdkonna arengu ja küberkuritegevusega;
- inimene ja õigus - õigusruum, inimese kohustused ja õigused;
- psühholoogia - psühholoogiline sõda, sotsiaalne manipulatsioon;
- füüsika ja tehnika - digitaalsed seadmed, andmete ülekanne, võrk;
- globaliseeruv maailm - veebipõhised andmebaasid, teabeallikad, majanduse areng ja inimtegevuse mõju;
- uurimustöö alused/arvuti kasutamine uurimistöös – teaduslik metoodika tegevuste planeerimises, analüüsis;
- rakenduste loomine ja programmeerimine – andmete sorteerimine, filtreerimine ja esitamine, analüüsimine;
- filosoofia - küsimuste äratundmine, küsimine, arutluskäikude koostamine, väärtused ühiskonnas, eetika.

4 Õppetegevuse kavandamine ja korraldamine

Õppetegevust kavandades ja korraldades:

- käsitletakse teemasid baastasemel ning võimalikult praktiliselt ja elulähedaselt; tuuakse näiteid reaalsest elust ja olukordadest Eestis ning mujal maailmas;
- lähtutakse õppekava alusväärtustest, üldpädevustest, õppeaine eesmärkidest, õppesisust ja oodatavatest õpitulemustest ning toetatakse lõimingut teiste õppeainete ja läbivate teemadega;
- lõimitakse teoreetilised teemad teiste õppeainetega (vt. Lõiming);
- tagatakse tulemus erinevate teemade kordamise ning järgnevate teemadega seoste loomise kaudu;
- õpilase õpikoormus (sh kodutööde maht) on mõõdukas, jaotub õppeaasta ulatuses ühtlaselt ning jätab õpilasele piisavalt aega läbitud teemade kinnistamiseks;
- võimaldatakse õppida individuaalselt ja üheskoos teistega (iseseisvad, paaris- ning rühmatööd), et toetada õpilaste kujunemist aktiivseteks ja iseseisvateks õppijateks ning loovateks ja kriitiliselt mõtlevateks isiksusteks, kes oskavad töötada ka meeskonnas;
- kasutatakse erinevaid õppemeetodeid, sh aktiivõpet: paaris- ja rühmatöö, vestlus, diskussioon, väitlus, arutelu, seminar, projektõpe, simulatsioon; skeemi, plaani, tabeli koostamine; praktilised ja uurimistööd; infootsing teabeallikatest ja infoanalüüs; referaadi ja ettekande koostamine; allikaanalüüs (dokument, tekst, statistika jms); töö erinevate e-riigi vahenditega (riigiportaal, e-teenused, teabepäring, õigusaktid internetis);
- kasutatakse diferentseeritud õppeülesandeid, mille sisu ja raskusaste toetavad individualiseeritud käsitlust ning suurendavad õpimotivatsiooni;
- rakendatakse nüüdisaegseid info- ja kommunikatsioonitehnoloogiatel põhinevaid õpikeskkondi ning õppematerjale ja -vahendeid;
- laiendatakse võimalusel õpikeskkonda: näitused, küberkaitsega seotud institutsioonide külastamine, võistlused, virtuaalmasinate kasutamine jne;

- ollakse sõltumatu tarkvaratootjast: õpe ehitatakse üles rohkem kui ühe tarkvaratootja või -platvormi kasutamisele. Kool peaks tutvustama vähemalt kaht erinevat tehnilist lahendust: arvuti operatsioonisüsteeme (nt MS Windows, macOS, GNU/Linux) ning samuti nutiseadmete operatsioonisüsteeme (nt Android, iOS, Windows Phone).

4.1 Hindamise alused

Hindamisel kasutatakse sõnalist mitteeristavat hindamist – „Arvestatud“ – „Mittearvestatud“.

Õpitulemusi hinnatakse E-portfoolio alusel.

E-portfoolio on personaalne veebipõhine keskkond (platvormi valib kool/õpilane ise), kuhu õpilane kogub kokkuvõtteid tunnis õpitud/ käsitletud teemade kohta (milliseid teemasid tunnis käsitleti, mida õppis jne). Õpiülesanded sooritatakse ja e-portfooliot peetakse kas üksi või rühmatööna; E-portfoolio on üldiselt avalik, aga peab võimaldama ka piiratud ligipääsuga sisu.

4.2 Nõuded füüsilisele keskkonnale

Kursusel osalemine eeldab järgmiste vahendite kasutamist:

- üldjuhul on igal õpilasel eraldi arvutitöökoht, kuid loenguid võib viia läbi ka arvutiteta ruumis;
- esitlusvahend (nt. dataprojektor);
- on failide salvestamise võimalus võrgukettale või kooli pakutavasse/ toetatud veebikeskkonda;
- on juurdepääs infosüsteemidele ja internetile (e-kool, intranet või veebipõhine sisuhaldussüsteem, rühmatöö keskkond, videoteek, e-koolikott);
- on kursuse läbiviimiseks on olemas tehniline baas nt. kõrvaklapid ja mikrofonid, võrguseadmed ning need vastavad kehtivale tervisekaitse nõuetele ja soovitustele jne;
- teised konkreetse valikõppeaine ainekavade läbi viimiseks on vajalikud vahendid: kirjanduse ja näidete kogum, eritarkvara vastavalt ülesannete iseloomule.

5 Ainekava

5.1 Õppe- ja kasvatuseesmärgid

Küberkaitse õppekavaga taotletakse, et õpilane:

- oleks Eestile lojaalne isik, kellel on positiivne hoiak ja valmidus vajaduse korral Eestit ja liitlasi kaitsta ning kes tegutseb lähtuvalt õigusriigi põhimõtetest;
- järgiks demokraatlikke väärtusi ning oleks vastutustundlik;
- mõistab küberkaitse seotust erinevate ühiskonnaelu valdkondadega ja tulevikutrendidega;

- teab Eesti e-riigi ning küberkaitse korraldust, e-riigi lahenduste ülesehituse põhimõtteid ning valdkondlikke õigusakte;
- teab küberkaitse, kõrgtehnoloogiliste konfliktide ning küberkuritegevuse ajalugu;
- on omandanud esmased oskused koduse IT-võrgu ja laiatarbeseadmete turvalisuse tagamiseks ning kaitsmiseks enamlevinud küberturbeintsidentide eest;
- tunneb digitaalse ohutuse aluseid (sh. isiku- ja tervisekaitse) ja kasutab neid teadlikult omaenda ja teiste turvalisuse tõstmiseks;
- hindab ja analüüsib vastuvõetavat infot kriitiliselt;
- oskab küberintsidenti kirjeldada ja dokumenteerida ning koostada asjakohase teatise pädevale ametiasutusele;
- oskab omandatud teadmisi ja oskusi rakendada praktikas ja tulevase eriala valikul.

Õpitulemus	Aeg	Õpisisu	Hindamise võimalus
SISSEJUHATUS INFOÜHISKONDA			Essee / arutelu
a. Oskab anda ülevaate digiühiskonna toimimisest	2	Digiühiskonna kultuur ja eetika; Infoühiskonna tehniline struktuur (taristu) näitena e-Eesti ülesehitus ja komponendid.	
b. Teab infoturbe ajalugu, tähtsamaid küberrünnakuid ning esimeste viiruste kirjutamise asjaolusid	2	Küberturvalisuse ajalugu ja intsidendid.	
c. Teab, selgitab ja rakendab küberkaitse ja küberkuritegevuse valdkonna põhimõisteid	2	**Mõisted:** Andmed, Andmekaitse, Andmekogu, Andmete töötlemine, Autoriseerimine, Avalik võti, Avarii (Disaster), Avatekst, Avatus (Exposure), Dark Web, Deep Web Dekrüpteerimine, Dešifreerimiseks, Ekstranet, Elutähtis teenus, Foori protokoll (Traffic Light Protocol), Küberkriminalistika (Forensics), Haavatavus (Vulnerability), Hübriidsõda, Identiteet, Identiteedi vargus, Identifitseerimine, Informatsioon, Infosüsteem, Infovara, Internet, Intranet, Intsident (Incident), IP aadress, Isikuandmed, Jadašifer (stream cipher), Käideldavus, Kaitsetus (Exposure), Konfidentsiaalsus, Krüpteerimine, Krüptoalgoritm, Krüptograafia, Krüptogramm, Küberkuritegu, Kübersõda, Lunavara (Ransomware), MAC aadress, Marsruuter, Nimeserver, Nõrkus (Vulnerability), Nuhkvara, Oht (Threat), Õngitsemine, Pahavara, Plokkšifer (block cipher), Probleem (Problem), Räsi, Risk, Ründeskript (exploit), Salajane võti, Seiresüsteem, Sertifikaat, Server, Šifreerimine, Signeerimine, Sündmus (Event), Terviklus, Trollid, Tulemüür, Turvaauk, Turvameede, Uss (worm), Vara (asset), Viirus, Virtuaalne privaatvõrk, Võrgulüüs **Lühendid:** 3DES, AES, ARP, AV, BYOD, CA, CERT, CHAP, CRC, DDoS, DES, DoS, EDI, ETO, FTP, FW, GMT, HIPAA, HMI, HTTP, IDEA, IDS, IMAP, IOT, IPS,	

		ISKE, ISO, LAN, MIME, NAT, NTP, OSINT, PAN, PAP, PCI-DSS, PGP, PKI, PLC, POP / POP3, RC4, RSA, S/MIME, SCADA, SMTP, SNMP, SSH, SSL, TCP, TLS, UDP, UTZ, VPN, WAN, WEP, WPA	
INFORUUM JA ANDMED			Juhtumite analüüs, praktilised ülesanded
a. Oskab kriitiliselt hinnata ja analüüsida teavet	1	Inforuum, info manipulatsioon.	
b. Eristab erinevaid küberpettuste tüüpjuhtumeid nende tagajärgede ja potensiaalse kahju järgi	2	Enamlevinud küberpettused: õngitsemine, petukirjad, petulehed, kontode kaaperdamine jne. Kuidas ära tunda pettust. Petulehtede ja -kirjade näidised	
c. Arvestab digitegevustes teiste inimeste privaatsusega ja isikuandmete kaitsmisega	2	Identiteet, Identimine, (mitmefaktoriline) autentimine ja autoriseerimine. Andmete kogumine, hoiustamine ja jagamine. Küberkiusamine	
d. Analüüsib ja esitab seisukohti ning toob näiteid tehnoloogiliste uuenduste mõju kohta inimeste elu- ja töökeskkonnale nii minevikus, tänapäeval kui ka tulevikus	2	IoT, Küberrünnak (ddos), eemaldamine (sh. piraatlus), sõltuvused, suurandmed (s.h. digitaalne jalajälg), globalne kontroll ja tsensuur; Tark maja	
SEADUSED JA REGULATSIOONID			Juhtumite analüüs-ühe tüüplepingu analüüs (meeskonnatööna)
a. Eristab seaduslikke ja ebaseaduslikke tegevusi toetudes IKT ja kübervaldkonda reguleerivatele seadustele, et kaitsta enda õigusi	2	Küberjulgeoleku õiguslikud alused (seadusandlik raamistik). EL digitaalne turg (kaupmees ja klient).	
b. Analüüsib erinevate organisatsioonide (nt 3 erinevat tüüpi) tüüptingimusi küberohutuse valdkonnas	2	Andmete kogumine ja kasutamine, Minu õigused ja kohustused (seadused). Avalikest allikatest (sh. sotsiaalmeedia) informatsiooni kogumine, kasutamine, mainekujundus (tööandja/töötaja), privaatsus asutuse sees,	

		küberkiusamine asutuses. Sotsiaalmeedia. Õigus olla unustatud.	
c. Selgitab ja väldib terviseriske seonduvalt digivahendite, digitehnoloogia (alates ergonoomika aspektidest kuni tehnoloogiasõltuvuseni) ja toob näiteid, kuidas digikeskkond võib muuta elu paremaks või halvemaks, lähtudes sellest, kuidas seda kasutatakse ja mis reegleid järgitakse	1	Tehnoloogia ja küberhügieeni alaste otsuste mõju keskkonnale, füüsilisele ja vaimsele tervisele. Eetika. Tuleviku trendid.	
MEETMED			Praktilised ülesanded + viib läbi turvaauditi (digikäitumise ja seadmete kasutamise osas)
a. Rakendab täiendavaid ohutus- ja turvameetmeid küberkeskkonnas	6	Seadmed meie ümber; tingmärgid, turvalisus. IP aadress, logi, kellaaeg, sündmuste korrelatsioon. IPv4 versus IPv6. Erinevad IT süsteemid ning kuidas on need seotud igapäevase eluga (telefon, e-post, Facebook, pangakaardid, tark tarneahel (EDI), X-tee jne)	
b. Teeb veaotsinguga kindlaks tehnilised probleemid ning leiab võimalikud lahendused	7	Pahavara, tulemüür, viirusetõrje, turvaline failide/programmide allalaadimine ja paikamine, võrgumured.	
c. Oskab kirjeldada ja dokumenteerida toimunud intsidenti ning koostada vastava teatise pädevale ametiasutusele	2	Logid. Abi leidmine nt. Veebikonstaabel, RIA, tarbijakaitse, andmekaitse inspektsioon, Lasteabi, IT-teadlik tuttav vms.	
ENESETÄIENDAMINE			Digipädevuste kaardistamine (Küberhügieeni test). Digipädevuste

			mudeli alusel hindamine
a. Hindab oma digipädevuse taset ja leiab puudujäägid oma teadmistes ning planeerib edasiõppimise võimalust	2	Edasiõppimise võimalused valdkonnas. Küberkaitsega seotud ametid. Karjääri planeerimine, õppimis- ja töötamisvõimalused, teadustöö / uurimistöö võimalused.	

5.2 Õppeprotsessi kirjeldus

5.2.1 Sissejuhatus infoühiskonda

Maht: 6 tundi (praktiline osa 2 tundi)

Teoreetiline osa: õppefilmi(de) vaatamine, mõistete tutvustamine, soovituslikule kirjandusele viitamine, slaidid / pildid

Praktiline osa: otsing ja kriitiline analüüs: uudised, võtmeisikud (nt Kevin Mitnick, Tõnu Samuel, Edward Snowden), juhtumid (nt IvyBells, Gunman, Venoma, GhostClick, StuxNet)

Hindamisvõimalus: essee / arutelu. Soovitame leida sobivad teemad õpisisu / küsimuste hulgast või materjalide põhjal.

Õpitulemus: *(a) Oskab anda ülevaate digiühiskonna toimimisest*

Õpisisu: Digiühiskonna kultuur ja eetika; Infoühiskonna tehniline struktuur (taristu) näitena e-Eesti ülesehitus ja komponendid.

Küsimused: Kuidas toimib infoühiskond? Kuidas on üles ehitatud infoühiskonna taristu (veebisirvijast serverini, e-Eesti näitel, sh side ja elekter)? Mis on digiühiskonna kultuuri ja eetika eripärad? Miks vajab infoühiskond kaitset?

Võimalikud materjalid: Anto Veldre "Infoühiskonnast hereetiliselt", lühiõppefilmid e-Eestist, Küberjulgeoleku strateegia.

Võimalikud esinejad: eksperdid KL KKÜ; teenusepakkujad (elekter, side); RIA

Õpitulemus: *(b) Teab infoturbe ajalugu, tähtsamaid küberrünnakuid ning esimeste viiruste kirjutamise asjaolusid*

Õpisisu: Küberturvalisuse ajalugu ja intsidendid.

Küsimused: Mis on küberkaitse ajaloo olulisemad verstapostid? Kus, miks ja kelle poolt luuakse pahavara? Kes oli Kevin Mitnick? Kes on osalejad ja mis on tüüpilised vastasseisud kübermaastikul?

Võimalikud materjalid: "Püramiidi tipus"; "Kübersõdalased" (õppefilmid); "War Games", "Hackers", "Die Hard 4" (iseseisvaks vaatamiseks); Kevin Mitnick raamat "The Art of Deception: Controlling the Human Element of Security" (õpetajale lugemiseks); RIA küberintsidentide aastaaruanded

Võimalikud esinejad: viirusetõrje / turbetehnoloogia firmade esindajad

Õpitulemus: *(c) Teab, selgitab ja rakendab küberkaitse ja küberkuritegevuse valdkonna põhimõisteid*

Õpisisu: Mõisted: Andmed, Andmekaitse, Andmekogu, Andmete töötlemine, Autoriseerimine, Avalik võti, Avarii (Disaster), Avatekst, Avatus (Exposure), Dark Web, Deep Web, Dekrüpteerimine, Dešifreerimiseks, Ekstranet, Elutähtis teenus, Foori protokoll (Traffic Light

Protocol), Küberkriminalistika (Forensics), Haavatavus (Vulnerability), Hübriidsõda, Identiteet, Identiteedi vargus, Identifitseerimine, Informatsioon, Infosüsteem, Infovara, Internet, Intranet, Intsident (Incident), IP aadress, Isikuandmed, Jadašifer (stream cipher), Käideldavus, Kaitsetus (Exposure), Konfidentsiaalsus, Krüpteerimine, Krüptoalgoritm, Krüptograafia, Krüptogramm, Küberkuritegu, Kübersõda, Lunavara (Ransomware), MAC aadress, Marsruuter, Nimeserver, Nõrkus (Vulnerability), Nuhkvara, Oht (Threat), Õngitsemine, Pahavara, Plokkšifer (block cipher), Probleem (Problem), Räsi, Risk, Ründeskript (exploit), Salajane võti, Seiresüsteem, Sertifikaat, Server, Šifreerimine, Signeerimine, Sündmus (Event), Terviklus, Trollid, Tulemüür, Turvaauk, Turvameede, Uss (worm), Vara (asset), Viirus, Virtuaalne privaatvõrk, Võrgulüüs

Lühendid: 3DES, AES, ARP, AV, BYOD, CA, CERT, CHAP, CRC, DDoS, DES, DoS, EDI, ETO, FTP, FW, GMT, HIPAA, HMI, HTTP, IDEA, IDS, IMAP, IOT, IPS, ISKE, ISO, LAN, MIME, NAT, NTP, OSINT, PAN, PAP, PCI-DSS, PGP, PKI, PLC, POP / POP3, RC4, RSA, S/MIME, SCADA, SMTP, SNMP, SSH, SSL, TCP, TLS, UDP, UTZ, VPN, WAN, WEP, WPA

Küsimused: Mis on infoturbe põhilised mõisted? Missugused on interneti legaalsed ja illegaalsed osad?

Võimalikud materjalid: Andmekaitse ja infoturbe leksikon [http://akit.cyber.ee/]; arvutikasutaja sõnaraamat [www.keeleveeb.ee]

Võimalikud esinejad: CERT, AKI, EISAÜ esindajad

5.2.2 Inforuum ja andmed

Maht: 7 tundi (praktilist osa 4 tundi)

Teoreetiline osa: õppefilmi(de) vaatamine, mõistete tutvustamine, soovituslikule kirjandusele viitamine, slaidid / pildid

Praktiline osa: Infomanipulatsiooni juhtumiga tutvumine ja selle analüüs (valitud juhtumi alusel analüüsib õpilane konflikti olemust, tuvastab osapooled ja nende arvatava motivatsiooni). Võimalusel potentsiaalse viirusega faili üleslaadimine virustotal.com lehele. Enda kohta info otsimine: (a) Ervinal [ervinal.eesti.ee]; (b) otsingumootorid (google, pipl, webmii). Erinevad rollid: mina, sõber, võõras. Erinevates maailma keeltes pildiotsingu tegemine (nt: relv, naine, surm, jne).

Hindamisvõimalus: juhtumite analüüs

Õpitulemus: *(a) Oskab kriitiliselt hinnata ja analüüsida teavet*

Õpisisu: Inforuum, info manipulatsioon.

Küsimused: Kuidas tuvastada pettust või kallutatud allikat / sisu? Kes toimivad inforuumis ja mis on nende võimalik motivatsioon?

Võimalikud materjalid: Allikad on ajakriitilised, tuleks kasutada aktuaalseid juhtumeid nii Eestis kui maailmas, Linnar Priimägi "Tõejärgse ajastu tõed"

Võimalikud esinejad: Raul Rebane (Stratkom OÜ), KV esindaja, KL esindaja, Riigikantselei esindaja, ajakirjanikud (Hans Lõugas, Henrik Roonemaa, Peeter Marvet), Jaak Aaviksoo, Ilmar Raag

Õpitulemus: *(b) eristab erinevaid küberpettuste tüüpjuhtumeid nende tagajärgede ja potentsiaalse kahju järgi*

Õpisisu: Enamlevinud küberpettused: õngitsemine, petukirjad, petulehed, kontode kaaperdamine jne. Kuidas pettust ära tunda. Petulehtede ja kirjade näidised.

Küsimused: Mis on küberpettus, missugust kahju see põhjustab? Kuidas vältida potentsiaalselt küberpettuse ohvriks sattumist?

Võimalikud materjalid: RIA blogi, veebikonstaablite ja politsei slaidid, blogi Propastop [www.propastop.org]

Võimalikud esinejad: Oskar Gross, veebikonstaablid, Anto Veldre, ülikoolide esindajad, KL KKÜ liikmed (blogi Propastop tegijad)

Õpitulemus: *(c) arvestab digitegevustes teiste inimeste privaatsusega ja isikuandmete kaitsega*

Õpisisu: Identiteet, identimine, (mitmefaktoriline) autentimine ja autoriseerimine. Andmete kogumine, hoiustamine ja jagamine. Küberkiusamine

Küsimused: Miks on privaatsus ja identiteet oluline? Kuidas saan muuta oma infosüsteemidesse sisenemist turvalisemaks? Miks piiratakse kasutajaõiguseid? Kuidas andmetega turvaliselt ringi käia? Mis on küberkiusamine ja kuidas sellega hakkama saada?

Võimalikud materjalid: Andmekaitse Inspektsiooni soovitused, Targalt Internetis veebileht, kampaania "Assapauk"

Võimalikud esinejad: Andmekaitse Inspektsioon, Sertifitseerimiskeskus, jne.

Õpitulemus: *(d) analüüsib ja esitab seisukohti ning toob näiteid tehnoloogiliste uuenduste mõju kohta inimeste elu ja töökeskkonnale nii minevikus, tänapäeval kui ka tulevikus*

Õpisisu: IoT, Küberrünnak (DDoS),eemaldamine (sh. piraatlus), suurandmed (s.h. digitaalne jalajälg), globaalne kontroll, tsensuur ja tehnoloogiline sõltuvus/abitus, EL digitaalne turg (kaupmees ja klient). Tark maja

Küsimused: Milliseid andmeid minu kohta kogutakse ja kuidas neid kasutatakse? Missugused väljakutsed, võimalused ja piirangud võivad tulevikus ühiskonda ees oodata?

Võimalikud materjalid: EL Andmekaitsedirektiiv (NIS Directive), A. Baum magistritöö, ervinal.eesti.ee, 'Andmejälgija'

Võimalikud esinejad: juristid (Karmen Turk, Eneken Tikk, Anna-Maria Osula), Heli Tiirmaa-Klaar, Luukas Ilves

5.2.3 Seadused ja regulatsioonid

Maht: 5 tundi, s.h. praktiline osa 3 tundi

Teoreetiline töö: seaduste tutvustamine, soovituslikule kirjandusele viitamine, slaidid / pildid

Praktiline töö: Tüüplepingute analüüs. Juhtumi alusel vastava seaduse paragrahvi leidmine. Väitlusülesanne. Tervise teema: sundasendite läbikatsetamine, harjutused nende vältimiseks.

Hindamisvõimalused: juhtumianalüüs

Õpitulemus: *(a) Eristab seaduslikke ja ebaseaduslikke tegevusi toetudes IKT ja kübervaldkonda reguleerivatele seadustele, et kaitsta enda õigusi*

Õpisisu: Küberjulgeoleku õiguslikud alused (seadusandlik raamistik).

Küsimused: Millised on minu õigused ja kohustused? Millised on digimaalima puudutavad seadused ja regulatsioonid? Mille poolest erinevad küberturve ja infoturve (suhtlemisvõimelised masinad, robotid)?

Võimalikud materjalid: Karistusseadustik. MKM veebileht. Hädaolukorra seadus. Pariseltkavoi.ee veebileht

Võimalikud esinejad: juristid, veebikonstaablid, KIIK kaitse eest vastutavad isikud.

Õpitulemus: *(b) Analüüsib erinevate organisatsioonide (nt 3 erinevat tüüpi) tüüptingimused küberohutuse valdkonnas*

Õpisisu: Andmete kogumine ja kasutamine, Minu õigused ja kohustused (seadused). Avalikest allikatest (sh. sotsiaalmeedia) informatsiooni kogumine, kasutamine, mainekujundus (tööandja/töötaja), privaatsus asutuse sees, küberkiusamine asutuses. Sotsiaalmeedia. Õigus olla unustatud.

Küsimused: Milliseid põhiõigusi võidakse regulatsioonidega piirata või laiendada? Missuguseid andmeid võib ettevõte minu kohta koguda ja avalikustada? Millised on minu seaduslikud võimalused organisatsioonis end kaitsta? Millised kokkulepitud lepitud reeglid ei kehti (riikliku julgeoleku huvid, erinevad seadused erinevates riikides, jne)?

Võimalikud materjalid: Eesti Vabariigi põhiseadus, erinevate ettevõtete infoturbe eeskirjad, ISKE.

Võimalikud esinejad: ettevõtete infoturbejuhid.

Õpitulemus: *(c) Selgitab ja väldib terviseriske seonduvalt digivahendite ja digitehnoloogiaga (alates ergonoomika aspektidest kuni tehnoloogiasõltuvuseni) ja toob näiteid, kuidas digikeskkond võib muuta elu paremaks või halvemaks, lähtudes sellest, kuidas seda kasutatakse ja mis reegleid järgitakse*

Õpisisu: Tehnoloogia ja küberhügieeni alaste otsuste mõju keskkonnale, füüsilisele ja vaimsele tervisele. Eetika. Tuleviku trendid.

Küsimused: Millised on ohud tervisele, kasutades digitaalseid vahendeid, tegutsedes digitaalses keskkonnas? Mida tähendab ja kuidas vähendada: digireostus (reklaamid) ja tootmisreostus keskkonnas?

Võimalikud materjalid: Tervisekaitse veebileht (ei ole materjale). Eetikakeskus TÜ juures.

Võimalikud esinejad: teadlased, Terviseamet, meditsiinivaldkonna spetsialistid.

5.2.4 Meetmed

Maht: 15 tundi, s.h. praktiline ja iseseisev töö 8 tundi

Teoreetiline töö: õppefilmi(de) vaatamine, mõistete tutvustamine, soovituslikule kirjandusele viitamine, slaidid / pildid

Praktiline töö: Võrguskeemi koostamine. IP aadressi kuuluvuse leidmine (Robtex, Hurricane Electric), ping, traceroute. Oma IP aadressi tuvastamine, päritolu määratlemine, muutmine. IP teisendamine teenusepakkujaks (AS number) ja seostamine teenusepakkuja riigikoodiga. Turvaauditi läbi viimine (digikäitumise ja seadmete kasutamise osas). Tavakasutaja seadme tulemüüri seadistamine, viirusetõrje installeerimine, viirusest seadme puhastamine ja faili kontrollimine, reklaami blokeerimine jne. Võrguliikluse uurimine ja süvauurimine.

Iseseisev töö (5 tundi): Turvaaudit annab võimaluse praktiseerida õpitut ja lisada kursusele õpilasi huvitavaid teemasid (toimuvast arusaamiseks ning seostamiseks on vaja dokumenteerimist ja jooniseid. Koduse/ asutuse arvutivõrgu kaardistamine).

Hindamisvõimalused: Turvaaudit ja praktilised ülesanded

Õpitulemus: *(a) Rakendab täiendavaid ohutus- ja turvameetmeid küberkeskkonnas*

Õpisisu: Seadmed meie ümber; tingmärgid, turvalisus. IP aadress, logi, kellaaeg, sündmuste korrelatsioon. IPv4 versus IPv6. Erinevad IT süsteemid ning kuidas on need seotud igapäevase eluga (telefon, e-post, Facebook, pangakaardid, tark tarneahel (EDI), X-tee jne).

Küsimused: Milliseid tehnilisi mõisteid pean teadma ja oskama rakendada, et selgitada küberkeskkonnas ohutus- ja turvameetmeid? Kuidas joonistan üles oma võrguskeemi? Millised seadmed kasutavad veel arvutivõrku (printer, külmkapp, lambipirn, auto, kaugloetav elektriarvesti, jne)? Millised teenused vajavad milliste portide avamist ja kuidas see mõjutab turvalisust? Mille poolest erinevad Eesti riigi alamdomeen ja Eestis paiknev ISP (kas Eesti tunnusega server paikneb Eestis)?

Võimalikud materjalid: ülikoolide ja kutsekoolide võrgukursus

Võimalikud esinejad: võrguadministraatorid, "targa maja" arendajad, TTÜ Mektory külastus

Õpitulemus: *(b) Teeb veaotsinguga kindlaks tehnilised probleemid ning leiab võimalikud lahendused*

Õpisisu: Viirus, tulemüür, viirusetõrje, turvaline failide/programmide allalaadimine ja paikamine. Võrgumured.

Küsimused: Milliseid kaitsemehhanisme pean teadma, et oma seadmeid ja süsteeme kaitsta, ning kuidas? Miks peab pidevalt tarkvara uuendama? Kuidas lahendan IP konflikti (s.h. võõras seade võrgus, ebakvaliteetne sideühendus, pistik)? Milliseid juhtumeid tüüpiliselt tuleb lahendada (võõrad, ebaotstarbekad ja sanktsioneerimata teenused)? Kuidas jagan turvaliselt internetti ja arvuti ressurssi?

Võimalikud materjalid: ülikoolide ja ettevõtete materjalid. Võrguseadmete (nt. wifi seadmed) dokumentatsioon. CISCO kursus. Mikrotik.

Võimalikud esinejad: Viirusetõrje ja tulemüüri müügiga tegelevad firmad. ISP. Veljo Haamer.

Õpitulemus: *(c) oskab kirjeldada ja dokumenteerida toimunud intsidenti ning koostada vastava teatise pädevale ametiasutusele*

Õpisisu: Logid. Abi leidmine nt. Veebikonstaabel, RIA, tarbijakaitse, andmekaitse inspektsioon, Lasteabi, IT teadlik tuttav vms

Küsimused: Millised logid on olemas, kuidas logid tekivad ja kuidas neid saab kasutada intsidendi tõestamisel? Millised on minu võimalused abi saamiseks ja kuhu pöörduda? Kuidas koostan intsidendi kirjelduse selle edastamiseks?

Võimalikud materjalid: RIA intsidendi vorm

Võimalikud esinejad: veebikonstaablid, RIA, tarbijakaitse, andmekaitse inspektsioon, Lasteabi. Aare Kirna, Tõnu Samuel.

5.2.5 Enesetäiendamine

Maht: 2 tundi, s.h. 1,5 tundi praktiline töö

Teoreetiline töö: õpetaja tutvustab erinevaid keskkondi ja võimalusi.

Praktiline töö: õppijate IKT pädevuste mudeli alusel enese hindamine, küberhügieeni test.

Hindamisvõimalused: õpilase enesehindamine

Õpitulemused:

a. Hindab oma digipädevuse taset ja leiab puudujäägid oma teadmistes ning planeerib edasiõppimise võimalust

Õpisisu: Edasiõppimise võimalused valdkonnas. Küberkaitsega seotud ametid. Karjääri planeerimine, õppimis- ja töötamisvõimalused, teadustöö / uurimistöö võimalused.

Küsimused: Millised on minu oskused täna? Millised on võimalused edasi arendamiseks?

Võimalikud materjalid: Õppijate IKT pädevuste mudel, Cybexer test, OSKA raport, Rajaleidja ametite andmebaas, ECDL, ISTE standard

Võimalikud esinejad: Rajaleidja, ülikoolide värbajad, kutsekoda