Küberkaitse III “Digiturvalisus ja krüptograafia”

1. Õppe- ja kasvatuseesmärgid

Valikkursusega taotletakse, et õpilane:

1) teab mis on infovarad;
2) oskab planeerida ja rakendada esmaseid meetmeid andmelekke ja andmekao vältimiseks;
3) teab põhilisi ründeid ning oskab neid ära tunda;
4) oskab rakendada meetmeid rünnete ennetamiseks, tuvastamiseks ning nende mõjude ning tagajärgede vähendamiseks;
5) oskab eristada olulisemaid teenuseid vähem olulisematest ning tagada olulisematele võrguressurss eelisjärjekorras;
6) oskab seada tuvastamise reegleid ning saata vastav info logisse, saata teavitusi. Oskab logist leida seoseid ning nende baasil võtta vastu otsuseid.

2. Kursuse lühikirjeldus

Kursuse põhiosad:

1) infovarad;
2) ohud;
3) infoturve;
4) rünnete ajalugu ja tunnused;
5) rünnete vastumeetmed;
6) arvuti riistvara komponendid;

Kursusel käsitletakse erinevaid infovaraga seotud mõisteid ja põhimõtteid. Tutvutakse ohtudega, mis tekivad infovara haldamisel ja vaadeldakse kuidas tagada infoturvet. Tutvutakse erinevate rünnete ja rünnete ajalooga. Õpitakse ära tundma põhiliste rünnete tunnusmärke. Vaadeldakse erinevaid meetmeid, kuidas ründeid ära hoida või neid takistada. Vaadeldakse krüptograafia ajalugu ja õpitakse tundma krüptograafia erinevaid liigitust. Lisaks eelnimetatud teemadele ja alateemadele õpitakse tundma ka arvutit.

3. Õppetegevus

Õppetegevus toimub tehnoloogiaklassis seminaride ja praktikumide vormis. Esmalt läbivad õpilased teoreetilise osa ja hiljem saavad praktiliselt proovida ja katsetada oma teadmisi kooli seadmetel, isiklikel seadmetel ning virtuaalmasinates.

4. Füüsiline õpikeskkond

Tehnoloogia klass on varustatud erinevate võrguseadmetega (PC, Switch, Router, virtuaalmasinad jms) ning õpilased saavad nendega praktikumide käigus lahendada erinevaid ülesandeid.

5. Hindamine

Valikaine „Digiturvalisus ja krüptograafia“ õpitulemuste hindamine lähtub gümnaasiumi riikliku õppekava üldosas ja teistes hindamist reguleerivates dokumentides toodud hindamisalustest.

Õpitulemuste kontrolli ja hindamise eesmärk on saada ülevaade õpitulemuste saavutatusest ja õpilase individuaalsest arengust ning kasutada saadud teavet õppe tulemuslikumaks kavandamiseks. Hinnatakse nii teadmisi ja nende rakendamise oskust kui ka üldpädevuste saavutatust, sh õpioskusi kirjalike ja praktiliste tööde ning praktiliste tegevuste alusel, arvestades õpilase teadmiste ja oskuste vastavust ainekava taotletavatele õpitulemustele.

Õpitulemusi hinnatakse sõnaliste hinnangute ja numbriliste hinnetega. Õpilane peab teadma, mida ja millal hinnatakse, milliseid hindamisvahendeid kasutatakse ja millised on hindamise kriteeriumid.

Kursuse hinne kujuneb iseseisvate- ja praktiliste tööde hinnetest.

Iseseisvateks töödeks on erinevad praktilised harjutused, mille käigus peab õpilane rakendama teoreetilisi teadmisi. Kontrollitakse ja hinnatakse õpilase teoreetilisi teadmisi, informatsiooni leidmist ja selle rakendamisoskust, loovust ja vormistuse korrektsust ning töö iseseisvat sooritust.

Teema ja õpitulemus	Maht	Õpisisu ja mõisted	Hindamine
Infovarad		Mis on infovarad? Infovarade käideldavus, terviklikkus ja konfidentsiaalsus. **Materjal:** https://goo.gl/iuJQgT, https://goo.gl/DCeEzo,	Isikliku infovara loomine
Oskab selgitada, mis infovara täpsemalt on ning teab, mis selle otstarve on.	5	Selgitatakse välja, millised infovarad on olemas. Lisaks räägitakse nende konfidentsaalsusest, seadusandlusest ning käideldavusest.	
Infoturve ja ohud		**Mõisted:** DOS, TDOS, reflection, phising, viirus, uss, õelvara, lunavara, andmeleke	**Esitlus:** Kuidas ohtusid neutraliseerida?
Selgitab oma sõnadega infoturbe olulisust ning seda, kuidas saab tagada seda vajaliku turvet. Lisaks turbele suudab nimetada enamlevinuid ohtusid infovarale.	5	Õpitakse tundma erinevaid infoturve liike, kuidas effektiivsemalt seda tagada ning kas seda üldse peaks tegema. Lisaks otsitakse võimalike ohuliike infovarale ning proovitakse leida võimalikud turvavariandid.	
Ründed infovarale		**Mõisted:** DNS, SMTP, juhtserver, register, startup, tasks, temp folder, võrgu skaneerimine.	**Esitlus:** Rünnetest läbi aegade; Rünnete tüübid; Kuidas ründeid eristada?
Teab rünnete ajalugu ning miks ründeid tehti. On võimeline eristama erinevaid ründetüüpe	5	Kasutades interneti, leitakse ründeid, mis on mõjutanud kolmandat osapoolt. Lisaks informatsioonile, vaadatakse videosid, mis selgitavad miks ründeid on tehtud ning mis kasu sellest on saadud.	

ning teab erinevate rünnete tunnuseid.			
Rünnete vastumeetmed		**Mõisted:** Root, user, krüptograafia, sümmeetriline krüptograafia, asümmeetriline krüptograafia, räsi, PKI, antiviirus, tulemüür, monitooring, IDS, IPS **Võimalikud lektorid:** Tartu Ülikooli lektor Kristjan Krips	
Oskab kaitsta iseend rünnete eest ning suudab aidata ka teisi. Oskab juhendada ka teisi ning aidata neid pahalaste eest.	5	Õpilane teab mis on krüptograafia ning tunneb selle ajalugu. Õpilane oskab vastavalt rünnakule valida sobiva vastumeetme. Õpilane teab kuidas vastavat infovara kaitsta (tulemüür, antiviitus, uuendused jms).	
Arvuti riistvara komponendid		**Mõisted:** GPU, CPU, Motherboard, RAM, ROM, HDD, SSD, BIOS, POST, PS/2, USB, FIREWIRE, VGA, HDMI, DVI, I/O devices, UPS, LCD, LED, IPS **Materjal:** https://goo.gl/QXvZCb	
Tunneb arvuti siseelu ning suudab eristada erinevaid komponente ja nende liike. On võimeline arvutit nullist kokku panema ning vajadusel ka hooldama nõuetekohaselt.	15	Õpitakse tööohutust (elekter, maandamine jne), õpitakse tundma tööriistu ning õigeid töövõtteid. Antakse lühitutvustus arvutis olevatest komponentidest ning pannakse kokku iseseisvalt arvuti.	

7. Õppeprotsessi kirjeldus

7.1. Infovarad

Maht: 5 tundi

Teoreetiline osa: Uuritakse milliseid infovarasid on IT maailmas olemas ning peale nende infovarade leidmise, uuritakse, milliseid infovarasid on igalühel endal olemas juba.

Prabiktiline osa: Isikliku infovara loomine.

Hindamisvõimalus: Isikliku infovara loomine.

Õpitulemus: Oskab selgitada, mis infovara täpsemalt on ning teab, mis selle otstarve on.

Õpisisu: Selgitatakse välja, millised infovarad on olemas. Lisaks räägitakse nende konfidentsaalsusest, seadusandlusest ning käideldavusest.

7.2. Infoturve ja ohud

Maht: 5 tundi

Teoreetiline osa: Interneti avarustest otsides leitakse erinevaid infoturve liike. Räägitakse ja arutletakse, kuidas on võimalik infoturvet kaitsta ning kas peaks kaitsma.

Praktiline osa: Ohuliikide otsimine

Hindamisvõimalus: Kuidas ohtusid neutraliseerida?

Õpitulemus: Selgitab oma sõnadega infoturbe olulisust ning seda, kuidas saab tagada seda vajaliku turvet. Lisaks turbele suudab nimetada enamlevinuid ohtusid infovarale.

Õpisisu: Õpitakse tundma erinevaid infoturve liike, kuidas effektiivsemalt seda tagada ning kas seda üldse peaks tegema. Lisaks otsitakse võimalike ohuliike infovarale ning proovitakse leida võimalikud turvavariandid.

7.1.3 Ründed infovarale

Maht: 5 tundi

Teoreetiline osa: Võimsamate ja mõjukamate rünnete kohta uurimine ning vastuse leidmine, miks seda tehti. Lisaks sellele, otsitakse ja arutletakse erinevate ründetüüpide osas ning proovitakse leida tunnuseid.

Praktiline osa: Esitlus (Rünnetest läbi aegade; Rünnete tüübid; Kuidas ründeid eristada?)

Hindamisvõimalus: Toimunud ründe (situatsiooni) analüüsimine, ettepanekud tulevikuks.

Õpitulemus: Teab rünnete ajalugu ning miks ründeid tehti. On võimeline eristama erinevaid ründetüüpe ning teab erinevate rünnete tunnuseid.

Õpisisu: Kasutades interneti, leitakse ründeid, mis on mõjutanud kolmandat osapoolt. Lisaks informatsioonile, vaadatakse videosid, mis selgitavad miks ründeid on tehtud ning mis kasu sellest on saadud.

7.1.4 Rünnete vastumeetmed

Maht: 5 tundi

Teoreetiline osa: Rünnetele vastumeetmete otsimine, seadmete turvalisus, seadmete monitooring ning seadmete krüpteerimine.

Praktiline osa: Rünnete otsimine, simuleeritud rünnetega tutvumine ning vastumeetmete leidmine.

Hindamisvõimalus: Kooli seadmete või virtuaalmasinate turvaliseks muutmine.

Õpitulemus: Oskab kaitsta iseend rünnete eest ning suudab aidata ka teisi. Oskab juhendada ka teisi ning aidata neid pahalaste eest.

Õpisisu: Internetis uurides leitakse parimaid vastumeetmed rünnetele, lisaks otsitakse parimad turvalahendused seadmetele, nii PC, smartphone ja tabletile. Süsteemselt Linux, Windows, iOS, Android.

7.1.5 Arvuti riistvara komponendid

Maht: 15 tundi

Teoreetiline osa: Arvuti komponentidega tutvumine (emaplaat, protsessor, mälu, videokaart, laienduskaardid). Lisaks komponentidega tutvumisele saadakse teada, milleks neid komponente vaja läheb ning kas arvuti ilma mõne komponentida ka töötaks.

Praktiline osa: Arvuti komplekteerimine (Arvuti komplekteeritakse võimalikult korralikult, kaabeldus on korralik, kaablid ei ripu kuskil ning ei käi vastu jahutust.)

Hindamisvõimalus: Praktiline töö (arvuti komplekteerimine)

Õpitulemus: Tunneb arvuti siseelu ning suudab eristada erinevaid komponente ja nende liike. On võimeline arvutit nullist kokku panema ning vajadusel ka hooldama nõuetekohaselt.

Õpisisu: Õpitakse tööohutust (elekter, maandamine jne), õpitakse tundma tööriistu ning õigeid töövõtteid. Lühitutvustus arvuti komponendidest ning iseseisvalt arvuti komplekteerimine.