Küberkaitse ja digiteenused

1. Õppe- ja kasvatuseesmärgid

Infoühiskond õppekavaga taotletakse, et õpilane:

1) oleks Eestile lojaalne isik, kellel on positiivne hoiak ja valmidus vajaduse korral Eestit ja liitlasi kaitsta ning kes tegutseb lähtuvalt õigusriigi põhimõtetest;
2) järgiks demokraatlikke väärtusi ning oleks vastutustundlik;
3) mõistab küberkaitse seotust erinevate ühiskonnaelu valdkondadega ja tulevikutrendidega;
4) teab Eesti e-riigi ning küberkaitse korraldust, e-riigi lahenduste ülesehituse põhimõtteid ning valdkondlikke õigusakte;
5) teab küberkaitse, kõrgtehnoloogiliste konfliktide ning küberkuritegevuse ajalugu;
6) on omandanud esmased oskused koduse IT-võrgu ja laiatarbeseadmete turvalisuse tagamiseks ning kaitsmiseks enamlevinud küberturbeintsidentide eest;
7) tunneb digitaalse ohutuse aluseid (sh. isiku- ja tervisekaitse) ja kasutab neid teadlikult omaenda ja teiste turvalisuse tõstmiseks;
8) hindab ja analüüsib vastuvõetavat infot kriitiliselt;
9) oskab küberintsidenti kirjeldada ja dokumenteerida ning koostada asjakohase teatise pädevale ametiasutusele;
10) oskab omandatud teadmisi ja oskusi rakendada praktikas ja tulevase eriala valikul.

2. Õpitulemused

Kursuse lõpul õpilane:

1) käitub küberkeskkonnas vastutustundlikult;
2) teab kõrgtehnoloogilise sõja arengu põhijooni ning oskab selgitada hübriidsõja mõju ja olemust; seletab näidete kaudu, kuidas kõrgtehnoloogiline sõjapidamine ja hübriidsõda on mõjutanud tänast arusaama sõjast;
3) teab mõistete digitaalne jalajälg ning küberhügieen tähendust ja oskab neid igapäevaste näidetega selgitada
4) tunneb tänapäeva arvutite komponente ning lisaseadmeid
5) oskab selgitada, mis on IT-maailmas viirus, uss, nuhkvara, mis on turvaauk ja exploit;

6) teab infoturbe ajalugu, esimeste viiruste tekkimist ning küberrünnakuid;
7) mõistab logimise ja logide ning dokumenteerimise olemust ja eesmärki, aeg (GMT).

3. Õppeaine kirjeldus

Kursus 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.

Kuruses saavad õpilased ülevaate infost ja infoturbest, tänapäeva ohtudest, kriisidest ja relvakonfliktidest ning rahvusvahelisest õigusest tehnoloogia seisukohast, kõrgtehnoloogilise sh hübriidsõja ajaloost, tehnoloogia tungimisest sõjapidamisse ning selle mõjust sõjapidamisse.

Kursus koosneks 10 teemaplokist:

1) sissejuhatus ainesse ja küberkaitsesse;
2) küberkaitse ajalugu ja tänapäevane hübriidsõda;
3) küberhügieen;
4) propaganda ja valeinformatsioon;
5) avalikest allikatest informatsiooni leidmine;
6) infovarad ja turvalisus;
7) küberkaitse ja infoturve;
8) digiteenused Eestis;
9) küberkaitse Eestis;
10) küberjulgeoleku õiguslikud alused.

4. Õppeaine lõiming teiste ainevaldkondadega

Infoühiskond on multidistsiplinaarne kursus, millel on tihedaid kokkupuutepunkte mitmete teiste gümnaasiumi õppekava õppeainetega:

1) *ühiskonnaõpetus* – kodanikukasvatus, riigikaitse korraldus, kaitseväe ja Kaitseliidu struktuur, Euroopa Liit, NATO ja ÜRO, rahvusvahelised kriisid ja konfliktid, Eesti kaitsepoliitika;
2) *üldajalugu* – sõjaajalugu, kriiside ja konfliktide tekkepõhjused ning tagajärjed, rahvusvahelised kriisid ja konfliktid, Euroopa Liit, NATO ja ÜRO;

3) *riigikaitseõpetus* – militaarstruktuurid, riigikaitse ülesehitus;
4) *eesti keel* – terminoloogia, töö juriidiliste tekstidega, suuline ja kirjalik eneseväljendusoskus;
5) *võõrkeeled* – terminoloogia;
6) *karjääriõpetus* - karjääri ja edasise õppimise planeerimine;
7) *majandus- ja ettevõtlusõpe* - ühiskonna toimemehhanismid, majanduse edukuse ja kahju seos digitaalse valdkonna arengu ja küberkuritegevusega;
8) *inimene ja õigus* - õigusruum, inimese kohustused ja õigused;
9) *psühholoogia* - psühholoogiline sõda, sotsiaalne manipulatsioon;
10) *füüsika ja tehnika* - digitaalsed seadmed, andmete ülekanne, võrk;
11) *globaliseeruv maailm* - veebipõhised andmebaasid, teabeallikad, majanduse areng ja inimtegevuse mõju;
12) *uurimustöö alused/arvuti kasutamine uurimistöös* – teaduslik metoodika tegevuste planeerimises, analüüsis;
13) *rakenduste loomine ja programmeerimine* – andmete sorteerimine, filtreerimine ja esitamine, analüüsimine;
14) *filosoofia* - küsimuste äratundmine, küsimine, arutluskäikude koostamine, väärtused ühiskonnas, eetika.

5. Hindamise alused

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

Õpitulemusi hinnatakse E-portfoolio, praktiliste ülesannete täitmise 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.

6. Õppetegevuse kavandamine ja korraldamine

Õppetegevust kavandades ja korraldades:

1) käsitletakse teemasid baastasemel ning võimalikult praktiliselt ja elulähedaselt; tuuakse näiteid reaalsest elust ja olukordadest Eestis ning mujal maailmas;

2) lähtutakse õppekava alusväärtustest, üldpädevustest, õppeaine eesmärkidest, õppesisust ja oodatavatest õpitulemustest ning toetatakse lõimingut teiste õppeainete ja läbivate teemadega;
3) lõimitakse teoreetilised teemad teiste õppeainetega (vt. Lõiming);
4) tagatakse tulemus erinevate teemade kordamise ning järgnevate teemadega seoste loomise kaudu;
5) õpilase õpikoormus (sh kodutööde maht) on mõõdukas, jaotub õppeaasta ulatuses ühtlaselt ning jätab õpilasele piisavalt aega läbitud teemade kinnistamiseks;
6) 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;
7) 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);
8) kasutatakse diferentseeritud õppeülesandeid, mille sisu ja raskusaste toetavad individualiseeritud käsitlust ning suurendavad õpimotivatsiooni;
9) rakendatakse nüüdisaegseid info- ja kommunikatsioonitehnoloogiatel põhinevaid õpikeskkondi ning õppematerjale ja -vahendeid;
10) laiendatakse võimalusel õpikeskkonda: näitused, küberkaitsega seotud institutsioonide külastamine, võistlused, virtuaalmasinate kasutamine jne;
11) 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).

Teema	Maht	Märksõnad	Tulem	Märkus
Sissejuhatus ainesse ja küberkaitsesse	1	Valikaine tutvustus, küberruum, võrgundus, teemade tutvustus, internet meie ümber ja elus, küberkaitse valdkonnad, küberruum vs igapäevane elu.	Teema lõppedes õpilane: ● mõistab, kui oluline on suhtuda küberruumis toimuvale igapäevase tegevusega sarnaselt, ● mõistab kolme olulist tegurit küberkaitse valdkonnas tavakasutajal, ● omab ülevaadet ainest	
Küberkaitse ajalugu ja tänapäevane hübriidsõda	3	esimesed küberrünnakud, suurimad rünnakud läbi ajaloo, küberrünnakute seos ajalooliste sündmustega, küberrünnaku avastamine, uued suunad küberkuritegevuses, „kübertaktika“, kaasaegne hübriidsõda, küberruum ning konventsionaalne ja mittekonventsionaalne sõjapidamine, laiapõhjalike riigikaitse, WannaCry, NoPetya, ja teised viimase paari aasta rünnakud, Snowden ja wikileaks ning selle mõju turvalisusele	Teema lõppedes õpilane: ● omab ülevaadet küberrünnakute „evolutsioonist“ seoses IT-arenguga ● teab küberkaitse/-rünnaku funktsiooni kaasaegses hübriidsõjas ● teab meetmeid ja tegevusi, kuidas vältida olukorda, et satutakse kolmanda osapoolena küberrünnaku osaliseks ● teab, kuidas käituda, kui tekivad kahtlused, et tema seadme abil toimub küberrünnaku ● mõistab oma rolli laiemas küberrünnakus, kuna just tema	Oluline on, et õpilane näeb ennast kui osa laiemast võrgustikust, kes suudab otseselt panustada turvalisusesse küberruumis. Arutelu, kas Snowdeni ja Wikileaks tegevus on korrektne või riigireetmine, kas nende kahe tegevus on õilis või oht julgeolekule.

			hooletuse tõttu võidakse rünnata kriitilise tähtsusega infosüsteeme	
Küberhügieen	2	Paroolide pikkus ja vahetamine, seadmete lukustamine, vanade tarkvarade kasutamise riskid, viirusetõrje puudumine, andmete varguse võimalused, andmed nutiseadmes ja tahvelarvutis, rakendustega seotud ohud, enda seadmete kaitsmine, enamlevinud õngitsuskirjad, lunavaraga seotud riskid, seadme või konto ülevõtmine, informatsiooni jagamine sotsiaalmeedias, videokõnede ohud, kübermaailma ja füüsilise maailma seosed	Teema lõppedes õpilane: ● mõistab, et õngitsuskirju saatev isik pole midagi muud kui taskuvaras, ● saab aru, et küberruumis andmete avaldamine ja nõusoleku andmine ei erine oma olemuselt toavõtmete andmise ja koduse aadressi jagamisega suvalisele vastutulijale ● pöörab edaspidi rakenduste alla laadimisel ja kasutamisel, mis andmeid vastav rakendus minu kohta kogub, ● teadvustab, kui ohtlik on küberhügieeni reeglite eiramine, ● mõistab tarkvara uuendamise vajadust.	Teema on rohkem arutelu õpilastega ning nende igapäevasest käitumisest küberruumis. Oluline on õpilasel mõista oma tegevuse rolli üldises küberturvalisuses. Moodul on osaliselt ka sissejuhatav osa järgnevatesse teemadesse.
Propaganda ja valeinformatsioon	2	Inforuum, propaganda, valeuudised, (strateegiline) kommunikatsioon, informatsiooni manipuleerimine, psühholoogiline kaitse, spinn, suhtekorraldus, infosõja taktika	Teema lõppedes õpilane: ● teab propaganda olemust ning kasutamise põhimõtteid ● teab kommunikatsiooni rolli kaasaegses infosõjas ● tunneb ära lihtsamad propagandaallikad internetis ● oskab hinnata esmasel tasandil allika tõesust	Teema läbimisel on oluline õpilaste iseseisev töö erinevate allikatega ning seal oleva informatsiooni analüüs koolitaja juhendamisel

Avalikest allikatest informatsiooni leidmine	4	Infovarad, avalikud allikad, OSINT, avalikud registrid Eestis, jälitustegevus, enda andmed Internetis, andmete kustutamine internetist, andmete kogumine, IP-aadress, MAC-aadress, jalajälg internetis	Teema lõppedes õpilane: ● teab informatsiooni kogumise ja hoidmise põhimõtteid ● oskab leida enda kohta käivat informatsiooni ning tuvastada selle päritolu ● teab tegevusi, kuidas oma andmeid internetist eemaldada ● teab avalikest allikatest pärit informatsiooni kasutamise reegleid ● teab ohtusid, mis kaasnevad informatsiooni levimisega sotsiaalmeedias ● oskab enda kohta informatsiooni leida nii avalikest allikatest kui ka registritest	Õpilastel on võimalus õpetaja juhendamisel erinevaid meetodeid ja vahendeid kasutades enda kohta käivat infot koguda ja mõelda, kuidas võiks küberkurjategija teda rünnata.
Infovarad ja turvalisus	4	Infovarad, infovarade konfidentsiaalsus, krüptograafia ja liigid, avaliku võtme krüptograafia (PKI), andmete krüpteerimine erinevad krüpteerimisvõimalused, aegumisest, krüpteerimine ID-kaardiga ning selle iseärasused, infovara terviklikkus ja käideldavus. ISKE	Teema läbides õpilane: ● teab infovarasid ning oskab selgitada mõisteid konfidentsiaalsus, terviklikkus ja käideldavus infovarade mõiste ● teab krüptograafia olemust ning selle kasutamist ● oskab krüpteerida andmeid ID-kaardiga (kui õpilastel on ID-kaart või digi ID) ● oskavad kasutada tunnis tutvustatud vabavaralisi krüptolahendusi oma igapäevases elus. ● oskab hinnata infovarade	Õpilased saavad proovida erinevaid enamlevinud krüpteerimise võimalusi ning võib olla ka ise luua krüpteerimisvõimalus ja koostavad esmase auditi oma igapäevaste andmete ja etteantud asutuste andmete kohta, määrates ISKE nõuded.

Küberkaitse ja infoturve	4	küberkaitse ja infoturve, infoturbe olemus ja sisu, erinevad pahavarad ja nende kasutamise eesmärgid, pahavarade toimimine, nakatumise tunnused, pahavarade eemaldamise võimalused, erinevad kaitsevõimalused , viirusetõrje, BigData, Darkweb	Teema läbides õpilane: ● oskab selgitada infoturbe olemust ● teab erinevaid pahavarasid ning nende toimet ● oskab kirjeldada pahavaraga nakatunud seadme iseloomulikke jooni ● teab erinevaid võimalusi pahavara eemaldamiseks seadmest ● oskab paigaldada viirusetõrje programmi ning teostada seadme puhastamist ning kaitset.	Praktiline harjutus, kus õpilane paigaldab seadmesse viirusetõrje programmi või rakenduse, seejärel kontrollib seadet ning vajadusel kõrvaldab pahavara.
Digiteenused Eestis	4	X-tee, riigi infosüsteemi arhitektuur, kohalike omavalitsuste infosüsteemid, elektrooniline identiteet, riigi infosüsteemi disainimine (EMTA või Maanteeameti näitel) seadused ja lepped,	Teema läbides õpilane: ● teab Eesti riigi infosüsteemi arhitektuuri ja toimimise põhimõttteid ● teab erinevaid elektroonilise identiteedi vahendeid ja oskab neid kasutada ● teab kasutajasõbraliku infosüsteemi tunnuseid ja arengut praktilise näite baasil ● teab olulisi nüansse infosüsteemide kasutajalepingutes ning seal olevadi õigusi ja kohustusi.	Vaadatakse erinevaid infosüsteeme ja nende arengut ja toimimise põhimõtet. Analüüsitakse erinevate keskkondade teenuslepinguid.

Küberkaitse Eestis	6	Küberkaitse korraldus Eestis, RIA, CERT, ETO, kriitiline taristu,, ründed Eesti asutuste vastu viimased 2 aastat, ettevõtte küberkaitse korraldus, asutuste külastus	Teema lõppedes õpilane: ● teab küberkaitset korraldavaid asutusi ning nende ülesandeid ● teab Eesti e-teenuste, ID-kaardi ja X-tee põhimõtteid turvalisuse seisukohast ● teab Riigi Infosüsteemi Ameti rolli Eesti küberkaitses. ● teab ülevaadet andmekeskuse toimimisest ja turvameetmetest ● on tutvunud kodulähedase ETO või kriitilise taristu omaniku küberkaitse korraldusega	Teema puhul on plaanitud 2 õppetundi ETO või kriitilise taristu omaniku õppeteis
Küberjulgeoleku õiguslikud alused	4	küberjulgeolekut käsitlevad õigusaktid (Eesti ja Euroopa), kasutaja õigused ja kohustused, küberrünnakust teavitamine, piraatlus, kiusamine, võrgu kasutamise piiramine, sotsiaalmeedia, kontode ülevõtmine, identiteedi vargus, veebi konstaabel	Teema lõppedes õpilane: ● teab seadusi ja õigusakte mis reguleerivad küberkaitsealast tegevust ● teab Eestis riiklikul tasandil küberkaitsega tegelevaid asutusi ning nende peamisi ülesandeid ● teab oma kohustusi küberkaitse vallas ning tagajärgi nende kohustuste mittetäitmisel	See on võimalus tutvuda mõne asukohalähedase ettevõtte või siis ameti küberkaitse korraldusega. Teema võib liita ka ekskursiooniga Tallinnasse ning seal tutvuda Riigi Infosüsteemi Ameti jne.
Lõputest	1	●	●	

KOKKU: 35

Põltsamaa Ühisgümnaasium
Veski 5, 48106, Põltsamaa linn, Põltsamaa vald
Tel: +372 77 51 175
info@poltsamaa.edu.ee