Õppekava	*KVA (kooli valikaine)*
Valdkond	*Riigikaitse*
Õppeaine	***Küberkaitse***
Kursuse nimetus	*Küberkaitse I*
Õpetamise aeg	*11. klass*
Eelduskursused	*Puuduvad*
Lõiming	• *eesti keel – töö terminoloogia ja tekstidega, suuline ja kirjalik eneseväljendusoskus;* • *filosoofia – küsimuste/teemade ja arutluskäikude äratundmine ja koostamine, ühiskondlikud väärtused ja eetika;* • *füüsika ja tehnika – internetivõrku ühendatud seadmed, internet, andmeliiklus;* • *globaliseeruv maailm – taristu paiknemine; teabeallikad, inimtegevuse mõju;* • *inimene ja õigus – küberkaitset reguleeriv seadusandlus, õigused ja kohustused;* • *karjääriõpetus – edasiõppimise ja karjääri planeerimine;* • *majandus- ja ettevõtlusõpe – ühiskonna toimemehhanismid, majanduse digitaalne areng, majandust mõjutav küberkuritegevus;* • *psühholoogia – psühholoogiline sõda, hübriidsõda, manipulatsioonid;* • *riigikaitse – riigikaitse ülesehitus, küberkaitse on tänapäeval kõige hõlpsamini kasutusele võetav luure- ja lahinguväli;* • *võõrkeeled – terminoloogia ja ainealaste tekstide/videotega tutvumine;* • *ühiskonnaõpetus – kodanikukasvatus, riigikaitse korraldus, kaitsepoliitika;* • *üldajalugu – kriiside ja konfliktide tekkepõhjused ja tagajärjed. Euroopa Liit, NATO ja ÜRO.*
Õppetöö korraldus	*35 tundi*
Kursuse eesmärk	*Küberkaitse kursuse eesmärk on õpetada õpilasi nägema kübermaailma plusse, miinuseid, ohte ja võimalusi neid ohte kahandada. Samuti mõtlema ennast kübermaailma kaitsja rolli, kas selleks tulevikus ise saamise mõttes või osates toetada neid, kes on tulevaste riigikaitsjate alluvuses/kaastöötajad ja täidavad seda rolli.*
Kursuse lühikirjeldus	*Küberkaitse on pidevalt arenev ja muutuv valdkond. Seda, mis oli eelmisel aastal, asendavad uuel aastal järgmised turvameetodid, on olnud uued rünnakud, on tõusnud ja langenud küberturvalisusega seotud olnud „inimtähti“. Seetõttu saab ainekavas kursuse sisu kirjeldada, kuid mitte peensusteni lahti kirjutada.* *Kursuse käigus õpetatakse õpilasi nägema, inimeste erinevaid lähenemisviise ja eelistusi infotehnoloogiaga seotud lahenduste otsimisel ja leidmisel. Samuti õpetatakse kursusel osalejaid nägema oma õpingukaaslaste pidetud andeid, üritatakse suunata õpilasi aktsepteerima erinevuste rikastavat mõju.*

	Küberkaitse õpetamisel räägitakse vajadusest teha koostööd ümbritsevate töötajatega. Koostöö harjutamiseks tehakse grupitöid. ***I. Inforuum ja -ühiskond ning küberkaitse (4 tundi)*** *Selleks, et saada teada, teab mis on inforuum ja kuidas seal käituda ise jätkusuutlikult arenedes:* • *tuletatakse meelde, kuidas toimis info liikumine enne internetti (suuline pärimus, telegramm, telefon, televiisori algusaastad, trükipress), interneti algusaastatel (esimesed vestlusruumid, telnet);* • *arutletakse, millisena õpilased sooviksid oma loodud inforuumi näha tagantjärele vaadates, või kas nad iga oma digitaalsesse inforuumi jäetud jälge (näiteks peopildid, kirjutatud tekst) sooviksid näidata täna ka oma vanaemale;* • *arutletakse mida kasulikku on tänapäeva inforuumist võimalik leida;* • *arutletakse mida on võimalik leida inforuumist, mis ei ole nii kasulik (või kas mõnikord ikka on kasulik ka?), küsitakse „miks?“.* • *Räägitakse tänapäeva küberrünnakutest, milliseid asutusi või riike, sh Eestit need on tabanud ja valitsuste, riikide jm erinevate reageerimisüksuste reaktsioonist küberrünnakute korral. Kui pikk on rünnaku avastamise aeg, reageerimisaeg, millest see sõltub.* ***II. Digiühiskond Eesti näitel (2 tundi)*** *Selleks, et tutvuda digiühiskonnaga, võetakse ette Eesti näide. Õpetaja rägib:* • *Eesti eripärast e-teenuste tugistruktuurist.* *Arutletakse:* • *millised digiteenused on Eestis riigi tasemel kättesaadavad;* • *milliseid neist teenustest saavad õpilased kasutada;* • *milliseid neist teenustest kasutavad õpilaste pereliikmed.* *Praktilise tööna kasutatakse veebilehte eesti.ee, õpilased uurivad sealt iseseisvalt, millised teenused olemas on. Õpilased mõtlevad ja arutavad oma pere liikmetega, milliseid teenuseid kasutatakse – pärast arutletakse seda ühiselt klassiruumis.* *Õpetaja räägib õpilastele erinevatest digiteenustest ning vajadusest neid kaitsta, tuuakse näiteid maailmast, kus digiteenused on saanud haavata (haiglate andmete krüpteerimine, Wikileaks jm andmebaasid) ning mida oleks saanud teha nende kaitsmiseks.* ***III. Digiühiskonna kultuur ja eetika (4 tundi)*** *Digiühiskonna kultuurist ja eetikast rääkides arutleb õpetaja õpilastega, millisel viisil digimaailmas suheldakse ja kas see peaks olema erinev või sarnane tavaelus üksteisega suhtlemisest:* • *arutletakse koos õpilastega nende endi ja nende eakaaslaste suhtlemist tänapäeva inforuumis (milliseid vahendeid kasutatakse, kas ja kuidas valitakse suhtluskaaslasi, kui vabalt end tuntakse);*

	• *räägitakse digiga seotud kooliülesannete õigest lahendamisest, millised on tähelepanu vajavad nüansid (funktsionaalne lugemine);* • *arutletakse piire, mida õpilastele on seadnud kool ja nende vanemad, mida nad ise seavad ja mida seab riik, mis on tänapäeval jälgitav ja kas on midagi, mis ei ole;* • *infomüra ja tõde/vale internetis;* • *saadakse teada, mis on valeuudis.* *Praktilise rühmatööna luuakse ise tõene uudis ja valeuudis, kantakse need ette ning teised rühmad peavad ära arvama, milline uudis on tõene ja milline on valeuudis.* ***IV. Seadused ja regulatsioonid (2 tundi)*** *Õpilased tutvuvad õpetaja juhendamisel Eesti digiühiskonnas kehtivate seadustega ja õpivad neid internetist leidma.* *Internetist leitakse üheskoos ja arutletakse seaduste üle:* • *Küberturvalisuse seadus.* • *Kaitseväe põhimäärus, § 14 Küberväejuhatusest.* • *Kaitseliidu kaasmise tingimused ja kord küberturvalisuse tagamisel.* • *EV Põhiseadus kui kõigi seaduste alustala.* ***V. Infoühiskonna areng ja tulevik (2 tundi)*** *Arutletakse :* • *uued ja arenevad tehnoloogiad, sh end ise juhtivad masinad (autod, lennukid, robotid);* • *küberkaitsega seotud riskid tehnoloogiate kasutamisel;* • *kas privaatsus on oluline? Millal ei ole?* *Grupitööd. Kui on valida, kes jääb ellu vältimatu kokkupõrke ajal, siis keda peaks isesõitev masin eelistama. Millised võiksid olla humanoidi õigused.* ***VI. Andmed ja identiteet (2 tundi)*** *Mis on isikuandmed. Arutluse alla võetakse digitaalne jalajälg, anonüümsus, privaatsus, krüpteerimine ja turvaline autentimine. Digikoristamine, milleks seda vaja on.* ***VII. Pettused ja kelmused (3 tundi)*** *Räägitakse, mis on kübermaailmas pettus, mis on kelmus.* *Mis on küberkuritegu ja selle tagajärjed omanikule (riik, füüsiline isik, eraisik) ja kurjategijale.* *Kes on küberkurjategija ja millist kasu ta saab, kuidas seda ära kasutab.* *Piraatlus, mis kasu on piraatveebilehtede pidajal ja mis kahju on allalaadijal ning digivara omanikul. Miks on vajalik autorikaitset.*

	Ründevektorid küberkaitses: • *kurjategijad otsivad viise, kuidas saab ära kasutada erinevate veebilehtede ja serverite jm turvanõrkusi oma kasuks;* • *inimeste manipuleerimine oma kasu saamise eesmärgil.* *Petukirjad, kuidas neid ära tunda ja mida teha nende vältimiseks. Sihitud rünnak.* *Veebilehtede, sh e-poodide turvalisus ja pettuse eesmärgil üles pandud e-poe tuvastamine.* ***VIII. Pahavara (2 tundi)*** *Mis on pahavara. Kuidas see satub seadmetesse.* *Õpilastele räägitakse, kuidas oma seadet turvata. Millele pöörata tähelepanu turvalisuse suurendamiseks ja pahavara vältimiseks. Milliseid pahavarasid on olemas. Kuidas saadakse pahavara, kuidas pahavara vastu võideldakse.* *Praktilise tööna õpilane töötab internetist otsitud info abil läbi isikliku seadme turvasätted, kaalutleb viirusetõrje kasutuselevõttu. Seejärel arutletakse, milliseid nõuandeid õpilased leidsid, kas kõik oli kasutatav, miks ei olnud (operatsioonisüsteemide jm erinevused, aegunud soovitused – millest enam ei piisa).* ***IX. Infrastruktuur, võrk ja selle turve (2 tundi)*** *Internetivõrgu infrastruktuuriga tutvumine:* • *OSI-mudel ja selle kihtide vaheline kommunikatsioon.* • *Kuidas jõuab õpilase seadmesse internet.* • *Kuidas saab internet meid ümbritsevasse õhku.* • *Kuidas jõuab internet Wifi seadmeni või GSM saatjani.* • *Tulemüürid.* • *Kuidas ona omavahel ühendatud erinevad serverid ja internetivõrgud (meralused kaablid jne).* *Ohud infrastruktuurile ja internetivõrgule. Ohtude vältimine, võrgu parandamine (näriline internetiühendust tagavas kaevus, kaevetööd).* ***X. Veebiründed, võrgulogid (2 tundi)*** *Käsurea tundmaõppimine, oma arvutis käsurea avamine, kasutamine, võrguandmete kättesaamine – milleks seda vaja on, kuidas on sellest igapäevaselt kasu.* *Õpilased teevad käsurea kasutamise ülesanded õpetajaga kaasa. Otsivad ise infot, kuidas käsurida kasutada ja oma käe järgi seada ().* *Ründe liigid (näiteks DDoS, Man-in-the-Middle, Dictionary attack), mida iga rünne endast kujutab, kas saab end kaitsta. Mille alusel, milliseid logisid ja kuidas saab koguda, sh Honeypot.*

	Õpilased kasutavad võrguanalüüsi tarkvara Wireshark ja leiavad selle logidest selleks tunniks määratud info. Määratud info sõltub sellest, millises internetivõrgus seadmega viibitakse. ***XI. Nutiturvalisus ja kodune turvaaudit (2 tundi)*** *Individuaalne töö. Õpilane koostab oma infovarade auditi:* • *millised seadmed on minu kodus seotud internetiga,* • *kas need seadmed on kaistud (füüsiline ligipääs ja tarkvarauuendused),* • *kuivõrd suur oleks omanikule ühe või teise infovara kaotsiminek.* *Individuaalse töö tulemusi arutatakse tunnis. Millised aspektid said õpilaste poolt kaetud, kas võimalikke kahjusid saab vähendada.* *Kodutööks jääb rääkida oma kodustele küberturvalisusest, koostades enda jaoks enne 1-2 A4 mahus materjali koos vähemalt ühe lingiga sobilikule (kellele kodus on vaja rääkida, lapsed, eakad, erineva teadmusega täiskasvanud jne) videole ja küberturvalisuse testile. Saata see materjal õpetajale. Järgmisel kohtumiskorral teeb õpetaja kokkuvõtte parimatest väljapakutud linkidest ja teksti sisust.* ***XII. Eeskujud ja antieeskujud (3 tundi)*** *Arutelu ajaloolistest eeskujudest, kas nad on positiivsed või negatiivsed.* *Ahmed Mohamedi kellaintsident. Lasta õpilastel otsida materjali selle intsidendi kohta. Mida nad selle noormehe ja tema pere kohta teada saavad, millised olid tema teole raktsioonid kooli ja ühiskonna poolt. (https://en.wikipedia.org/wiki/Ahmed_Mohamed_clock_incident)* *Arutelu, kas Ahmed sai sellest intsidendist rohkem kasu või kahju. Millised olid tema teo tagajärjed.* *Edward Snowden, millised olid tema tegude tagajärjed. Mida õpilased oleks teinud, või kuidas lahendanud paremini Snowdeni ees seisnud probleemi.* *Suurfirmade küberkaitse süsteemid ja kaitsjad.* *Olukord küberruumis, viimase aja ründed, kui kiiresti neid märgati, kes on olnud nende taga, mida ründajad on kätte saanud. Kes ründajatest on kätte saadud ja millised nn vastase taristu osad on maha võetud.* ***XIII. Küberkaitse kompetentsid (2 tundi)*** *Küberkaitse kompetentse tutvustavas tunnis on lisaks õpetaja jutule hea kutsuda ka külalisesineja, kes oskab rääkida küberkaitsjale olulistest oskustest, teadmistest ja isikuomadustest. Seda praktiku seisukohast.* *Küberkaitse kompetentsist rääkides tuleb puudutada riigikaitses juhtival kohal oleva inimese suutlikkust ja soovi olla kursis ja toetada küberturvalisuse tegevusi. Sinna kuulub:*

	• *valmisolek toetada töötajate harimist küberhügieeni küsimustes,* • *enda kurssi viimine riskidega, mis ohustavad organisatsiooni edukat toimimist ja* • *vajadust pöörata digikeskkondade programmeerimisel tähelepanu nende turvalisusele.* *Samuti inimfaktoriga arvestamine ja krüpteerimise olulisuse rõhutamine.* *Räägime lühidalt krüptograafiast.* ***XIV. Õppimine ja karjäär küberkaitse vallas (3 tundi)*** *Igal õppeaastal viib õpetaja end kurssi õpilaste võimalustega küberkaitse vallas infot saada, kus end harida ja millised on perspektiivid karjäärile erinevate hariduse astmetega, erinevate spetsialiteetidega, sest küberkaitse on lai valdkond. Üks inimene ei jõua tegeleda kõigi küberkaitse valdkondadega, seega tuleb kindlasti valida endale õppesuund. Samuti on tekkinud massiliselt erinevaid e-õppeprogramme, mille seast valimiseks tuleb õppurile anda vähemalt mõned juhtnöörid (kui tuntud on õpet pakkuv asutus, kas e-õppe baasil on võimalik reaalselt saavutada kooli reklaamitud tulemust – või pakutakse, et saab ainult kolme tunnise õppega professionaaliks).*
Kursuse õpitulemused	*Kursuse läbinud õpilane:* *1) teab mis on inforuum ja kuidas seal käituda ise jätkusuutlikult arenedes;* *2) teab Eesti digiühiskonna ülesehitust ja oskab vajaduse korral nõu ja abi otsida, õpilane on aktiivne ja vastutustundlik digiühiskonna liige;* *3) oskab vahet teha, kes on ebasoovitav häkker ja kes on eetiline häkker, mis on digikultuur;* *4) teab Eesti digiühiskonnas kehtivaid seaduseid ja oskab neid internetist leida;* *5) tajub ja teadvustab ümbritsevat teabekeskkonda, saab aru selle pidevast muutumisest ning teab hetkel planeeritavaid tulevikusuundi; teadvustab füüsilise aktiivsuse mõju oma mõistuse teravana hoidmisel;* *6) saab aru isiklike andmete hoidmise vajadusest ning saab aru, mida tema kohta internetist on võimalik leida;* *7) teab digitaalse pettuse meetodeid ja oskab nendega arvestada;* *8) teab, mis on pahavara ja meetodeid sellest hoidumiseks;* *9) teab, kuidas on üles ehitatud internetivõrk ja miks seda on vaja turvata;* *10) teab, miks rünnatakse veebilehti, rakendusi ja võrke ning kuidas hoida neid turvatuna;* *11) teab, kuidas oma nutiseadmeid turvata; mõistab enda kodu kui ühiskonnarakukese olulisust küberturbes;*

	12) suudab ümbritsevat teabekeskkonda kriitiliselt analüüsida ning toimida selles oma eesmärkide ja ühiskonnas omaksvõetud kommunikatsioonieetika järg; *13) on kursis erinevate küberkaitsega seotud kompetentsidega;* *14) teab karjäärivõimalusi küberkaitses ja vajadust (potentsiaalse) juhina kaitsta Eesti IT taristut;* *15) on saanud kogemuse küberkaitsealastes grupitöödes osavõtust ja saab aru oma seisukohtade väljendamise olulisusest.*
Hindamisviis	*Õpilane on läbinud kursuse arvestatult, kui ta on osalenud aktiivselt vähemalt 21 tunnis.* *Hindamisel lähtutakse vastavatest gümnaasiumi riikliku õppekava üldosa sätetest. Hindamine küberkaitses tähendab konkreetsete õpitulemuste saavutatuse ja õppija arengu toetamist, kusjuures põhirõhk on õpilase arengu toetamisel. Hinnatakse õpilase teadmisi ja oskusi suuliste vastuste (esituste), kirjalike ja/või praktiliste tööde ning praktiliste tegevuste alusel, arvestades õpilase teadmiste ja oskuste vastavust taotletavatele õpitulemustele. Kirjalikke ülesandeid hinnates arvestatakse töö sisu. Õpitulemuste hindamisel kasutatakse sõnalisi hinnanguid ja numbrilisi hindeid. Õpilane peab teadma, mida ja millal hinnatakse ning milliseid hindamisvahendeid kasutatakse ja millised on hindamise kriteeriumid.* *Hindamise põhiülesanne on toetada õpilase arengut, et kujuneks arusaamine erinevate nii riigi kui isiklikus kasutuses olevate infosüsteemide ja nendega seotud infovarade turvaliselt ja eesmärgipäraselt kasutamise kohta rõhuga küberturvalisusel.* *Küberkaitse kursusel hinnatakse õpilaste teadmisi ja oskusi, kuid ei hinnata hoiakuid ega väärtusi. Hoiakute ja väärtuste kohta antakse õpilasele tagasisidet ja arutletakse nende üle eesmärgiga ehitada õpilases üles seaduskuulekas käitumisjoon.* *Õpitulemuste hindamise vormid on mitmekesised, sisaldades tagasisidet suulistele, kirjalikele ja praktilistele ülesannetele.* *Suuliste ja kirjalike ülesannete puhul õpilane:* *1) selgitab ning kirjeldab mõistete sisu ja omavahelisi seoseid;* *2) selgitab oma arvamusi, hinnanguid, seisukohti ja suhtumisi, seostades neid omandatud teadmistega;* *3) eristab, rühmitab, võrdleb ja analüüsib olukordi, tegevusi ning tunnuseid lähtuvalt planeeritud õpitulemustest;* *4) demonstreerib faktide, mõistete ning seaduspärasuste (tegevused ja tagajärjed) tundmist lähtuvalt õpiülesannete sisust.* *Praktiliste ülesannete puhul õpilane:*

	5) õpib õpetaja juhendamisel leidma vajalikke käske, töövahendeid, meetodeid, lahendusi oma seadme turvamisel; *6) rakendab teoreetilisi teadmisi praktiliselt õpisituatsioonis;* *7) demonstreerib õpitulemustes määratud oskusi õpisituatsioonis;* *8) kirjeldab õpitulemustes määratud teadmiste ja oskuste rakendamist igapäevaelus.*
Õppekirjandus Õppematerjalid Lisamaterjalid Lingid	*Mitmete teemade käsitlemisel kasutatakse Moodles olevat kursust, mis baseerub veebiõpikul Küberkaitse (B.Lorenz et al) https://web.htk.tlu.ee/digitaru/kyberkaitse/* *Kursuse käigus hoitakse õpilasi pidevalt kursis uute küberohtude ja rünnetega ning võimalustega ennast ja oma seadmeid kaitsta, kasutades info paremaks edasiandmiseks sel hetkel aktuaalseid veebilehti jm näitlikustavat materjali.* *Õppekirjandus:* • *Lorenz et al. Digiteenused. Informaatika valikkursus gümnaasiumile. https://web.htk.tlu.ee/digitaru/digiteenused/ (28.01.2021)* • *Lorenz et al. Küberkaitse. https://web.htk.tlu.ee/digitaru/kyberkaitse/ (28.01.2021)* • *CCDCOE. Publications. https://www.ccdcoe.org/library/publications/ (28.01.2021)* • *Eesti Informaatikaõpetajate selts. Küberkaitse ainekava: https://1drv.ms/w/s!AuRLzcD9FVl7ywlqPX-J4ewoLgIy (28.01.2021)* • *Küberturvalisus | COVID-19 kriisi veebileht. https://www.kriis.ee/et/kuberturvalisus (28.01.2021)* • *Riigi Infosüsteemi amet. https://www.ria.ee (28.01.2021)* • *Riigi Infosüsteemi amet. IT-vaatlik. https://itvaatlik.ee/ (28.01.2021)* • *Turvalisus Archives – Digitark. https://digitark.ee/teemad/turvalisus (28.01.2021)*
Vastutav õppetool	*Riigikaitse õppetool*
Kursuse väljund	*Ettevalmistus uurimistööks ja küberkaitse võistlusteks.*