Õppekava	*KVA (kooli valikaine)*
Valdkond	*Riigikaitse*
Õppeaine	***Küberkaitse***
Kursuse nimetus	*Küberkaitse II*
Õpetamise aeg	*11. klass*
Eelduskursused	*Küberkaitse I*
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 II kursuse eesmärk on anda õpilasele läbi praktiku silmade ülevaade küberkaitsest riigikaitse osana.*
Kursuse lühikirjeldus	*1. Küberkaitse ajalugu ja tänapäevane hübriidsõda* *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* *2. Propaganda ja valeinformatsioon* *Inforuum, propaganda, valeuudised, (strateegiline) kommunikatsioon, informatsiooni manipuleerimine, psühholoogiline kaitse, spinn, suhtekorraldus, infosõja taktika* *3. Avalikest allikatest informatsiooni leidmine* *Infovarad, avalikud allikad, OSINT, jälitustegevus, enda andmed Internetis, andmete kustutamine internetist, andmete kogumine, IP-aadress, MAC-aadress, jalajälg internetis*

	4. Infovarad ja turvalisus *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.* *5. Küberkaitse ja infoturve* *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* *6. Uue seadme kasutuselevõtt* *Uue seadme kasutuselevõtt, vajalikud tarkvarad ja seadistused, operatsioonisüsteem, viirusetõrje, kasutajaliidesed, õigused, varukoopiad, seadete ja andmete taastamine, andmete sünkroniseerimine, rämpsposti ja reklaami peatamine, seadme puhastamine,* *7. Turvaline võrk ja seadmed kodus* *Erinevad võrgud (Wifi, 3G/4G, LAN), avalikud Wifi võrgud, ohud ebaturvalises võrgus, ohud koduses võrgus, olmetehnika ja võrguühendus, asjade internet (IoT), kodused võrguseadmed, nende turvalisus, logid, võrguliikluse jälgimine ja uurimine* *8. Nutiseadmete turvalisus* *Nutiseadmete operatsioonisüsteemid, turvaaugud, nutiseadmed, turvaaukude avastamine ja lappimine* *9. Küberkaitse Eestis* *Küberkaitse korraldus Eestis, RIA, CERT, ETO, kriitiline taristu, X-tee, ründed Eesti asutuste vastu viimased 2 aastat, ettevõtte küberkaitse korraldus, ISKE* *10. Küberjulgeoleku õiguslikud alused* *küberjulgeolekut käsitlevad õigusaktid (Eesti ja Euroopa), kasutaja õigused ja kohustused, küberrünnakust teavitamine, piraatlus, kiusamine, võrgu kasutamise piiramine, sotsiaalmeedia, kontode ülevõtmine, identiteedi vargus, veebi konstaabel* *11. Asutuste külastamine* *Küberväejuhatus, USA väekoondise esindajad Eesti kohtumine, KL Küberkaitseüksus, Sisekaitseakadeemia.*
Kursuse õpitulemused	*Kursuse 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 hooletuse tõttu võidakse rünnata kriitilise tähtsusega infosüsteeme* • *teab propaganda olemust ning kasutamise põhimõtteid* • *teab kommunikatsiooni rolli kaasaegses infosõjas* • *tunneb ära lihtsamad propagandaallikad internetis* • *oskab hinnata esmasel tasandil allika tõesust* • *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* • *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 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.* • *standardtegevusi, et võtta uus seade turvaliselt kasutusele,* • *oskab paigaldada seadmesse vajalikke rakendusi* • *oskab varundada, kopeerida ja taastada andmeid erinevates seadmetes* • *teab ohtusid, mis tulenevad ebaturvalise võrgu kasutamisel,* • *oskab kasutada turvaliselt avatud Wifi võrku* • *teab, kuidas oma kodust võrku turvalisemaks muuta,* • *oskab muuta koduste võrguseadmete seadistusi nii, et on tagatud elementaarne turvalisus* • *teab programme ja rakendusi, mis aitavad tuvastada rünnakuid võrgust ning oskab neid rakendada* • *teab erinevate operatsioonisüsteemide eeliseid ja puudusi* • *teab erinevate nutiseadmete probleeme ja turvaauke,* • *oskab otsida turvaauke ja nende lappimise võimalusi* • *oskab otsida erinevatest allikatest lahendusi probleemidele* • *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 ehk kriitilise taristu omaniku küberkaitse korraldusega* • *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* *Pärast asutuste külastusi õpilane:*

	• *omab paremat ülevaadet küberkaitsega tegelevate asutuste igapäevatööst* • *on saanud esitada küsimusi küberkaitsega tegelevatele inimestele* • *oskab paremini teha edasiõppimiseks erialavalikut*
Hindamisviis	*Õpilane on läbinud kursuse arvestatult, kui ta on osalenud aktiivselt vähemalt 21 tunnis.* *Õpitulemuste hindamiseks läbib õpilane kursuse lõpus ainetesti.* *Hindamisel lähtutakse vastavatest gümnaasiumi riikliku õppekava üldosa sätetest. Hindamine küberkaitses tähendab konkreetsete õpitulemuste saavutatuse ja õppija arengu toetamist, kusjuures põhirõhk on õpilase arengu toetamisel.* *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.*
Õppekirjandus Õppematerjalid Lisamaterjalid Lingid	*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.* *Õppekirjandust annavad erinevad praktikud-lektorid.*
Vastutav õppetool	*Riigikaitse õppetool*
Kursuse väljund	*Ettevalmistus uurimistööks ja küberkaitse võistlusteks.*