Valikaine „Küberkaitse“ ainekava

Maht: 35 tundi

Eesmärgid: Tutvustada õpilastele küberkaitse olemust ja erinevaid distsipliine, pakkudes neile algteadmisi selles valdkonnas. Kursus loob aluse turvalise küberkeskkonna põhimõtete mõistmiseks, arendab õpilaste turvateadlikkust ning valmistab neid ette kogukondliku küberturvalisuse teadlikkuse tõstmise toetamiseks.

Õppekeskkond: Internetiühendusega klassiruum koos arvutitega, igale õpilasele personaalne arvuti, esitlusvahendiks projektor. Õppetegevuses on vaja õpilasel kasutada nutitelefoni.

Õppetegevus: keskendub õpilastele kübermaailma plusside, miinuste, ohtude ja nende vähendamise võimaluste tutvustamisele. Õpilasi julgustatakse mõtlema end kübermaailma kaitsja rolli, olgu see siis tulevikus ise küberkaitsjaks saamise või tulevaste riigikaitsjate toetamise mõttes. Küberkaitse õpetamisel rõhutatakse koostöö olulisust ümbritsevate töötajatega, mida harjutatakse grupitööde kaudu. Õpilasi õpetatakse mõistma, et inimestel on erinevaid lähenemisviise ja eelistusi infotehnoloogiaga seotud lahenduste leidmisel. Kursusel osalejaid julgustatakse nägema oma kaasõpilaste andeid ja aktsepteerima erinevuste rikastavat mõju. Arvestades, et küberkaitse on pidevalt arenev ja muutuv valdkond, toob iga aasta kaasa uusi turvameetodeid ja rünnakuid.

Õppesisu:

- Inforuum ja -ühiskond ning küberkaitse
- Digiühiskond Eesti näitel
- Digiühiskonna kultuur ja eetika
- Seadused ja regulatsioonid
- Infoühiskonna areng ja tulevik
- Andmed ja identiteet
- Pettused ja kelmused
- Pahavara
- Infrastruktuur, võrk ja selle turve
- Veebiründed, võrgulogid
- Nutiturvalisus ja kodune turvaaudit
- Eeskujud ja antieeskujud
- Küberkaitse kompetentsid
- Õppimine ja karjäär küberkaitse vallas

Õpitulemused

- teab mis on inforuum ja kuidas seal käituda ise jätkusuutlikult arenedes;
- teab Eesti digiühiskonna ülesehitust ja oskab vajaduse korral nõu ja abi otsida, õpilane on aktiivne ja vastutustundlik digiühiskonna liige;
- oskab vahet teha, kes on ebasoovitav häkker ja kes on eetiline häkker, mis on digikultuur;
- teab Eesti digiühiskonnas kehtivaid seaduseid ja oskab neid internetist leida;
- tajub ja teadvustab ümbritsevat teabekeskkonda, saab aru selle pidevast muutumisest ning teab hetkel planeeritavaid tulevikusuundi; teadvustab füüsilise aktiivsuse mõju oma mõistuse teravana hoidmisel;
- saab aru isiklike andmete hoidmise vajadusest ning saab aru, mida tema kohta internetist on võimalik leida;
- teab digitaalse pettuse meetodeid ja oskab nendega arvestada;

- teab, mis on pahavara ja meetodeid sellest hoidumiseks;
- teab, kuidas on üles ehitatud internetivõrk ja miks seda on vaja turvata;
- teab, miks rünnatakse veebilehti, rakendusi ja võrke ning kuidas hoida neid turvatuna;
- teab, kuidas oma nutiseadmeid turvata; mõistab enda kodu kui ühiskonnarakukese olulisust küberturbes;
- suudab ümbritsevat teabekeskkonda kriitiliselt analüüsida ning toimida selles oma eesmärkide ja ühiskonnas omaksvõetud kommunikatsioonieetika järg;
- on kursis erinevate küberkaitsega seotud kompetentsidega;
- teab karjäärivõimalusi küberkaitses ja vajadust (potentsiaalse) juhina kaitsta Eesti IT taristut;
- on saanud kogemuse küberkaitsealastes grupitöödes osavõtust ja saab aru oma seisukohtade väljendamise olulisusest.

Hindamine
Mitteeristav hindamine - arvestatud või mittearvestatud. Hindamisel lähtutakse gümnaasiumi riikliku õppekava üldosa sätetest, keskendudes õpilase arengu toetamisele ja konkreetsete õpitulemuste saavutamisele. Küberkaitse kursusel hinnatakse teadmisi ja oskusi, kuid hoiakuid ja väärtusi ei hinnata, nende kohta antakse tagasisidet.

Õpitulemusi hinnatakse e-portfoolio alusel, kuhu kogutakse tehtud praktilised tööd. Kursusel on võimalus teha ka miniteste (H5P) ja pikemaid teste, mida saab kasutada iseseisva hindamise tööriistana (eelhindamine ja järelhindamine), mitte hindelise tööna. Kursusel on ka 1-2 pikemat ankeeti, milles saab oma oskusi sügavamalt analüüsida kursuse alguses ja lõpus.