

Valikkursus Küberkaitse

Kursuse nimetus	Küberkaitse
Eelduskursus	SG valikkursus „Informaatikas alused“, „Programmerimise alused“ ja „Programmeerimine“
Kursuse läbiviimise aeg	G3, I pa
Kursuse maht	20 tundi * 75 min + 2 tundi iseseisvat tööd
Kursuse eesmärgid	Gümnaasiumi informaatika valikkursuse „Küberkaitse“ eesmärgiks on anda õpilastele ettekujutus küberkaitse olemusest ja distsipliinidest ning võimaldada neil omandada algteadmised antud valdkonnas. Ainekavas sisalduva õppetegevuse kaudu omandatakse küberkaitse valdkonna üldised teadmised, mis kinnistatakse praktilise tegevuse kaudu. Õppeaine eesmärk on panna alus turvalise küberkeskkonna põhimõtete mõistmisele, kujundada õpilaste turvateadlikkust ja valmisolekut vajaduse korral toetada kogukondliku küberturvalisuse teadlikkuse tõstmist. Küberkaitse 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. Küberhügieen on käesoleva õppeaine kontekstis defineeritud kui kasutaja poolt asjakohaste turbemeetmete kasutusele võtmine IT-süsteemide ja seadmete kasutamisel ning küberturvalisuse parimate praktikate järgimine.
Kursuse lühikirjeldus (õppetegevus)	Õppetegevust kavandades ja korraldades: 1) käsitletakse teemasid baastasemel ning võimalikult praktiliselt ja elulähedaselt; tuuakse näiteid reaalsest elust ja olukordadest Eestis ning mujal maailmas; 2) lõimitakse teoreetilised teemad teiste õppeainetega; 3) tagatakse tulemus erinevate teemade kordamise ning järgnevate teemadega seoste loomise kaudu; 4) kasutatakse erinevaid õppemeetodeid, sh aktiivõpe: nt paaris- ja rühmatöö, vestlus, diskussioon, väitlus, arutelu, seminar, projektõpe, simulatsioon; skeemi, plaani, tabeli koostamine; praktilised tööd ja uurimistööd; infootsing ja -analüüs; referaadi ja ettekande

	koostamine; allikaanalüüs (dokument, tekst, statistika jms); töö erinevate e-riigi vahenditega (riigiportaal, e-teenused, teabepäring, õigusaktid internetis); 5) kasutatakse diferentseeritud õppeülesandeid, mille sisu ja raskusaste toetavad individualiseeritud käsitlust ning suurendavad õpimotivatsiooni; 6) laiendatakse võimaluse korral õpikeskkonda: näitused, küberkaitsega seotud institutsioonide külastamine, võistlused, virtuaalmasinate kasutamine jne; 7) 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).
Lõiming teiste õppeainetega	Küberkaitse kursus lõimitakse teiste õppeainetega mitmel viisil, järgides kooli õppekava ja õpetamismetoodika põhimõtteid: Matemaatika ja statistika: Õpilased analüüsivad andmeid ja kasutavad matemaatilisi mudeleid, et mõista küberkuritegevuse statistikat ja turvameetmete tõhusust. Ajalugu ja ühiskonnaõpetus: Kursus tutvustab küberkaitse ajalugu ja sotsiaalseid mõjusid, sealhulgas seaduste ja regulatsioonide mõju digitaalses maailmas. Keel ja kirjandus: Õpilased koostavad referaate ja ettekandeid, analüüsivad küberkaitsealast kirjandust ning kasutavad tõlgendusoskusi küberohutuse kontekstis. Tehnoloogia ja infotehnoloogia: Kursus tutvustab erinevaid operatsioonisüsteeme ja platvorme (näiteks Windows, macOS, Android, iOS), samuti IT-süsteemide turvalisuse põhimõtteid ja parimaid tavasid. Kunst ja disain: Õpilased võivad luua küberkaitsega seotud visuaalseid projekte või kujundada infograafikat, mis selgitab küberohutuse kontseptsioone ja protsesse. Praktilised tegevused ja ekskursioonid: Kursuse raames korraldatakse külastusi küberkaitsega seotud institutsioonidesse ja osaletakse võistlustel, et laiendada õpikeskkonda ja rakendada õpitut reaalses olukordades.
Õppekäigud/projektid	-

Õpioskuste arendamine	Õpioskuste arendamine küberkaitse kursusel toimub mitmeti: Praktiline õpe ja simulatsioonid: Õpilased lahendavad praktilisi ülesandeid ja simulatsioone, mis simuleerivad reaalseid küberohtusid ja -rünnakuid. See arendab nende probleemilahendamise oskusi ja võimet reageerida kriitilistes olukordades. Kriitiline mõtlemine ja analüütilised oskused: Õpilased õpivad analüüsima küberohte ja hindama turvariske erinevates stsenaariumides. See arendab nende võimet teha informeeritud otsuseid ja rakendada turvameetmeid. Koostöö ja meeskonnatöö: Grupiprojektid ja ülesanded julgustavad õpilasi töötama koos teistega, jagama ideid ja leidma lahendusi küberkaitse väljakutsetele koos meeskonnaga. Tehnoloogilised oskused: Õpilased arendavad praktilisi tehnilisi oskusi, sealhulgas turvaanalüüsi tööriistade kasutamist, võrgu skaneerimist ja haavatavuste hindamist. Kommunikatsioon ja teadlikkuse tõstmine: Õpilased õpivad selgelt väljendama turvameetmete vajalikkust ja edendama kogukondlikku küberturvalisust. See hõlmab ka suhtlemisoskuste arendamist ja teadlikkuse tõstmist küberohtudest.
Kursuse õpitulemused (konkreetne kursus)	Küberkaitse õppekavaga taotletakse, et õpilane: 1) on Eestile lojaalne isik, kellel on positiivne hoiak ja valmidus vajaduse korral Eestit ja liitlasi kaitsta ning kes tegutseb lähtuvalt õigusriigi põhimõtetest; 2) järgib 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) valdab lihtsamaid võtteid 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) kirjeldab ja dokumenteerib küberintsidendi ning koostab asjakohase teatise pädevale ametiasutusele; 10) rakendab küberkaitse-alaseid teadmisi ja oskusi tulevase eriala valikul.
Hindamine sh lõpptulemuse kujunemine	Hindamisel lähtutakse Sillamäe Gümnaasiumi õppekava üldosa sätetest. Valikkursust „Küberkaitse“ hinnatakse Sillamäe Gümnaasiumis protsendilisel skaalal lähtudes õpilaste teadmiste ja oskuste tasemest. Sellise hindamise eesmärk on anda selgemat, õiglasemat ja sisulisemat tagasisidet õpitulemuste saavutamise kohta. Hindamine tugineb vastavalt riiklikus õppekavas ja kooli ainekavas määratletud õpitulemustele ning hindamiskriteeriumitele alljärgneva protsendilise skaala alusel. Protsendiline hindamisskaala, õpilane: 90–100% – saavutas kõik või peaaegu kõik õpiväljundid väga hea arusaamine juures, lahendused on täpsed ja loogilised, õpilasel on oskus rakendada teadmisi uutes olukordades. 75–89% – saavutas enamiku õpiväljundeid; teadmised on korrektsed ja oskused valdavalt tasemel, kuigi esinevad üksikud ebatäpsused keerukamates ülesannetes 51–74% – saavutas osaliselt õpiväljundid; saab ainekavast aru, kuid esinevad märgatavad vead või ebatäpsused lahenduskäigus < 50% – ei saavutanud nõutud õpiväljundeid; arusaamine käsitletud teemadest on puudulik ning esinevad olulised vead lahendustes Valikaine õpitulemusi hinnatakse jooksvalt ja kontrolltöö õpiülesannete järgi, ja kokkuvõtvalt kursuse lõpul üldjuhul e-portfoolio abil. E-portfoolio on personaalne veebipõhine keskkond, millesse õpilane kogub pikema perioodi jooksul enda tehtud tööd ja refleksioonid oma õpikogemustest. Hinnatakse:

	1) õppe plaanipärasust, loomingulisust ja ratsionaalsust; 2) õppekavas ettenähtud õpitulemuste saavutamist ning seonduvate pädevuste olemasolu veenvat tõendamist õpilase poolt; 3) arvutiga loodud materjalide tehnilist teostust, esteetilisust ning originaalsust; 4) õpilasepoolset praktilise tegevuse mõtestamist; 5) õpilase arengut. Kursusehinde moodustavad 3 kontrolltööd digiõpiku kohta + KüberPuuring ja Kobras võistlused (kui nad toimuvad samal ajal kursusega): 1) Infoühiskond 2) Risk ja oht 3) Edasiõppimine ja karjäär Täpsem hindamismudel on õpilastele alati kättesaadav Stuudiumi kaudu õppeaine info alt. Lisaks tutvustab õpetaja hindamispõhimõtteid kursuse esimeses tunnis ning enne iga olulisemat hinnatavat tööd, et tagada õpilastele selgus ja õiglane ootuste mõistmine.
Õppematerjalid	Veebikeskkond https://www.targaltinternetis.ee/ CTF Tech portaal https://ctftech.com/
Soovituslik kirjandus	Küberkaitse https://web.htk.tlu.ee/digitaru/kyberkaitse/
Kursuse väljund (lõpptulemus mitme kursuse korral)	Kursuse "Küberkaitse" läbinud õpilased suudavad mõista ja rakendada kriitilisi küberkaitse põhimõtteid, tagades süsteemide konfidentsiaalsuse, tervikluse ja kättesaadavuse. Neil on oskus hinnata ja leevendada küberohte, kasutades praktilisi turvameetmeid ja teostades haavatavuste analüüsi. Õpilased suudavad selgelt selgitada küberkaitse seadusandlust ja eetilisi aspekte ning edendada kogukondlikku teadlikkust küberohutusest. Kursus varustab õpilasi vajalike oskuste ja teadmistega, et jätkata edasist õppimist küberkaitse valdkonnas ja panustada digitaalses maailmas turvalisuse tagamisse.