

Mikrokvalifikatsiooniõppe õppekava vorm täienduskoolitusasutustele

1. ÜLDANDMED (kohustuslikud väljad on tähistatud tärniga *)

Täienduskoolitusasutuse nimetus*	Tallinna Tehnikaülikool
Õppekava nimetus (eesti keeles)*	Küberohud, tehisintellekt ja pahavara
Õppekava nimetus (inglise keeles)*	Cyber Threats, AI and Malware
Õppe liik* - mikrokvalifikatsioon - mikrokraad (kõrgkoolid saavad liigitada, kui õppekavast 50% on kõrgharidusõppeained)	mikrokraad
Õppekavarühm* (lähtutakse täienduskoolituse standardist, liigitamisel on abiks käsiraamat https://www.hm.ee/sites/default/files/documents/2022-11/kehtiv_01.01.2017_isced-f-2013.pdf)	Tarkvara ja rakenduste arendus ning analüüs
Õppe maht ainepunktides* (1 AP = 26 tundi õppija tööd, mis sisaldab nii õppekeskkonnas toimuvaid tegevusi kui ka iseseivat tööd)	21 EAP
Õppekeel*	Inglise keel
Sihtrühm ja/või õppe alustamise tingimused (nt suunatud teatud valdkondade töötajatele, nõutav eelnev haridus, teatud töökogemus või erioskused, spetsiifilised teadmised või ettevalmistus)	Küberturbe valdkonna töötajad.
Lõpetamise tingimused* eksam/arvestus ja osalemise % (kui kehtib)	Eksamite ja arvestuste sooritamine positiivsele tulemusele.
Õppekava koostamise alus (nt koostatud formaalõppe, kutsestandardi või selle osa, teatud õigusakti jms alusel)	Koostatud IVSB17 Küberturbe tehnoloogiaste õppekava alusel
Õppekava vastavus EKR-le (Eesti kvalifikatsiooniraamistiku taseme lisamine on kohustuslik kõrgkoolidele ja kutseõppeasutustele; täienduskoolitusasutused ei pea seda märkima)	tase 6

2. ÕPPEKAVA EESMÄRK JA ÕPIVÄLJUNDID*

Õppekava eesmärk (kirjeldab õpiväljundeid kokkuvõtva lausena)	Pakkuda õppijale terviklikud teadmised ja praktilised oskused küberohtude tuvastamiseks, analüüsimiseks ja käsitlemiseks, kombineerides kaasaegseid
--	---

	seire- ja logihalduslahendusi, intsidentide halduse metoodikaid ning tehisintellekti rakendusi küberturbe kontekstis.
Õppekava õpiväljundid* (kirjeldavad teadmisi ja oskusi, mida õppija õppeprotsessi lõpuks omandab, tavaliselt on iga õppekava puhul 4-6 peamist õpiväljundit)	1. Selgitab küberturbe intsidentide elutsüklit ning rakendab asjakohaseid protsesse ja dokumentatsiooni intsidentide tõhusaks haldamiseks.
	2. Rakendab logimise ja süsteemiseire põhimõtteid, kasutades tsentraliseeritud lahendusi ning analüüsimeetodeid ohtude tuvastamiseks ja seireks.
	3. Analüüsib ja tuvastab küberohte, kasutades tehisintellekti ja masinõppe meetodeid, sealhulgas anomaaliade tuvastamist ja kahjurvara klassifitseerimist.
	4. Rakendab turvameetmeid veebirakendustes, mõistes levinumaid ründemehhanisme ning osates valida ja kasutada sobivaid kaitsevõtteid.
	5. Hindab küberturbe lahenduste, sh tehisintellekti kasutuselevõtu riske, turvalisust ning eetilisi ja privaatsusaspekte.

3. ÕPPEPROTSESSI KIRJELDUS*

3.1 ÕPPE SISU, ÕPPEMEETODID, MAHU JAOTUS*

Teema/moodul/aine (kui õppeainel või moodulil on eraldi õpiväljundid, tuleb need siia lisada)	Õppemeetod(id) (kontaktõpe, veebipõhine õpe, hübriidõpe)	Mahu jaotus (kontaktõpe sh praktiline töö, iseseisev töö, muu)
ICS0032 Intsidentide haldus Õppeaine läbinu: - kirjeldab intsidentide halduse protsessi / elutsüklit ja selle osasid; - koostab intsidentide halduse dokumentatsiooni ja aruandeid; - nimetab, millised on asjakohased tööriistad intsidentide halduses.	kontaktõpe	Loengud 2 x 16 = 32 t Praktikumid 2 x 16 = 32 t ja 92 tundi iseseisev õpe

<p>ICS0037 Tehisintellekt küberturbes Õppeaine läbinu: - selgitab tehisintellekti ja masinõppe põhimõisteid ning nende seoseid küberturvalisusega; - rakendab tehisintellekti ja masinõppe meetodeid ohtude tuvastamiseks ning analüüsimiseks, sealhulgas anomaaliate tuvastamine, kahjurvara klassifitseerimine ja õngitsuskatsete tuvastamine; - paigaldab ja kasutab TI-põhiseid tööriistu ohujahiks, intsidentidele reageerimiseks ja turvatoimingute automatiseerimisel; - analüüsib ja oskab kaitsta TI süsteeme vaenulike rünnakute eest ning mõista TI omaseid turvariske; - hindab TI kasutuselevõtu eetilisi ja privaatsuse tagamise aspekte.</p>	<p>kontaktõpe</p>	<p>Loengud 2 x 16 = 32 t Praktikumid 2 x 16 = 32 t ja 92 tundi iseseisev õpe</p>
<p>ICS0028 Kurivara Õppeaine läbinul on: - nimetab erinevaid kurivara liike; - hindab ja valib vahendeid kurivara tuvastamiseks; - rakendab ennetavaid meetmeid.</p>	<p>kontaktõpe</p>	<p>Loengud 1 x 16 = 16 t Praktikumid 1 x 16 = 16 t ja 46 tundi iseseisev õpe</p>
<p>Valida üks kahest õppeainest: ICS0020 - Logimine ja süsteemiseire või ICS0027 Veebirakenduste turvalisus valida ICS0020 Õppeaine läbinu oskab: - määratleda sobivat lähenemisviisi keskse seire ja logimislahenduse ning</p>	<p>kontaktõpe</p>	<p>Loengud 2 x 16 = 32 t Praktikumid 2 x 16 = 32 t ja 92 tundi iseseisev õpe</p>

analüütika rakendamisel; - töötada platvormilogidega Linux/Windows keskkonnas; - määratleda ja rakendada logimise nõuded rakendustes ning skriptides; - rakendada tsentraliseeritud logihalduslahendust; - rakendada tsentraliseeritud seirelahendust; - töötada rsyslog platvormiga; - teostada korrelatsiooni; - määratleda seire ja logihalduse jaoks vajalikud tööprotsessid		
ICS0027 Veebirakenduste turvalisus Õppeaine läbinu: - nimetab levinuimaid veebirakenduste ründemeetodeid ja neid puudutavaid põhimõisteid, - loetleb veebirakenduste levinuimaid kaitsevõimalusi, - kasutab veebirakenduste levinuimaid kaitsevõimalusi praktikas veebiteenuste juures	kontaktõpe	Loengud 2 x 16 = 32 t Praktikumid 2 x 16 = 32 t ja 92 tundi iseseisev õpe

3.2 ÕPPEKESKKONNA KIRJELDUS (võib olla nii füüsilise kui ka veebipõhine)*

<i>Kus ja kuidas õppetöö toimub – füüsiliselt kohapeal, veebis või hübriidõppena? Millised õppekeskkonna võimalused on õppijale tagatud, sh seadmed ja vahendid? Kas õppekoht on ligipääsetav kõigile? Mida peab õppija ise kaasa võtma või omama (nt sülearvuti, nutitelefon, tarkvara lahendus jne)?</i>	Õppetöö toimumine on õppeainetes erinev. Õppetööd viiakse läbi IT kolledži ruumides kohapeal, aga ka veebis (Teams) ja hübriidõppena. Loengud on osaliselt eelsalvestatud, nii kohapeal kui veebis toimub õppetöö üldjuhul salvestatakse. IT kolledži õpperuumidesse on hea ligipääsetavus, parkimisvõimalused on maja lähedal. Üliõpilastel on soovitatav omada sülearvutit.
--	--

3.3 ÕPPEMATERJALIDE LOETELU

<i>Õppetöös kasutatav kohustuslik kirjandus, sealhulgas raamatud, õpikud, teemakohased käsiraamatud, teadusartiklid, asjakohased veebiallikad jne.</i>	Tööks kasutatavate materjalide loetelu on esitatud iga õppeaine ainekaardis.
--	---

4. HINDAMINE JA VÄLJASTATAVAD DOKUMENDID*

4.1 Hindamine* (sisaldab hindamismeetodeid ja -kriteeriume)

Hindamismeetodid	Hindamiskriteeriumid	Hinnatavad õpiväljundid
Lisame iga aine lõpphindamise meetodi ja selle kriteeriumid. Nimetame õpiväljundi (1, 2,3...), mida hindame nende meetoditega.		
ICS0032 Intsidentide haldus Rühmatöö ja eksam	Rühmatöö vastab nõutud kriteeriumidele. Eksam sooritatakse positiivsele tulemusele.	1. kirjeldab intsidentide halduse protsessi / elutsükli ja selle osasid; 2. koostab intsidentide halduse dokumentatsiooni ja aruandeid; 3. nimetab, millised on asjakohased tööriistad intsidentide halduses.
ICS0037 Tehisintellekt küberturbes Iseseisev töö ja eksam	Iseseisev töö vastab nõutud kriteeriumidele. Eksam sooritatakse positiivsele tulemusele.	2. rakendab tehisintellekti ja masinõppe meetodeid ohtude tuvastamiseks ning analüüsimiseks, sealhulgas anomaaliade tuvastamine, kahjurvara klassifitseerimine ja õngitsuskatsete tuvastamine; 4. analüüsib ja oskab kaitsta TI süsteeme vaenulike rünnakute eest ning mõista TI omaseid turvariske; 5. hindab TI kasutuselevõtu eetilisi ja privaatsuse tagamise aspekte.
ICS0028 Kurivara Eksam	Eksam sooritatakse positiivsele tulemusele.	1. arusaamine erinevatest kurivara liikidest; 2. oskus valida vahendeid kurivara tuvastamiseks; 3. oskus rakendada ennetavaid meetmeid.
ICS0020 - Logimine ja süsteemiseire – valikaine Eksam	Eksam sooritatakse positiivsele tulemusele.	1. lähenemisviisi keskse seire ja logimislahenduse ning analüütika rakendamisel; 2. töötada platvormilogidega Linux/Windows keskkonnas; 3. määratleda ja rakendada logimise nõuded rakendustes ning skriptides; 4. rakendada

		tsentraliseeritud logihalduslahendust; 5. rakendada tsentraliseeritud seirelahendust; 6. teostada korrelatsiooni ja määratleda seire ja logihalduse jaoks vajalikud tööprotsessid.
ICS0027 Veebirakenduste turvalisus Arvestus	Projektitöö vastab nõutud kriteeriumidele ja arvestus sooritatakse ettenähtud nõuetele.	Õppeaine läbinu: 1. nimetab levinuimaid veebirakenduste ründemeeetodeid ja neid puudutavaid põhimõisteid, 2. loetleb veebirakenduste levinuimaid kaitsevõimalusi, 3. kasutab veebirakenduste levinuimaid kaitsevõimalusi praktikas veebiteenuste juures.

4.2 Väljastatavad dokumendid*

Mikrokvalifikatsiooni tunnistus

5. KOOLITAJATE KVALIFIKATSIOONI ÜLDINE KIRJELDUS* (Milline haridus, kvalifikatsioon või töökogemus on koolitajatel nõutav? Lisaks erialasele pädevusele peab koolitajatel olema ka täiskasvanute koolitamise oskus. Samuti märkida koolitajate eeldatav arv ning võimalusel lisada nende nimed, kui need on kindlalt teada.)

<i>Üldsõnaline kompetentside kirjeldus, õppejõud, kes sel hetkel õpetavad.</i>
<i>Koolitaja eeldatav haridustase, seos õppejõu või lektori atesteerimisega (sh viimane atesteerimise kuupäev)</i>
<p><i>Küberohud, tehisintellekt ja pahavara praktikule</i> mikrokraadi õppejõudude kvalifikatsioon on tagatud Tallinna Tehnikaülikooli akadeemilistele töötajatele esitatavate nõuetega.</p> <p>ICS0032 Intsidentide haldus õppejõud Neeme Kalda, Tallinna Ülikooli infotehnoloogia juhtimise õppekava, MSc.</p> <p>ICS0037 Tehisintellekt küberturbes õppejõud Margus Ernits, TalTech ja Tartu Ülikooli küberkaitse ühisõppekava, MSc.</p> <p>ICS0028 Kurivara õppejõud Maria Schlosser, TalTech küberturbe tehnoloogia õppekava, BSc.</p> <p>ICS0020 - Logimine ja süsteemiseire või ICS0027 Veebirakenduste turvalisus</p> <p>Õppejõud Ali Ghasempour, TalTech ja Tartu Ülikooli küberkaitse ühisõppekava, MSc.</p> <p>Kõikidel õppejõududel on ettevõtluses töötamise kogemus.</p>