Ida-Virumaa Kutsehariduskeskuse õppekava

26.02.2020 kinnitatud 26.02.2020

Õppekavarühm	Andmebaaside ja võrgu disain ning haldus					
Õppekava nimetus	IT-turvaspetsialist					
	ICT Security Specialist					
Õppekava kood EHISes	215071					
ESMAÕPPE ÕPPEKAVA					JÄTKUÕPPE ÕPPEKAVA	
EKR 2	**EKR 3**	**EKR 4 kutsekeskharidus**	**EKR 4**	**EKR 5**	**EKR 4**	**EKR 5**
						X
Õppekava maht (EKAP):	60					
Õppekava koostamise alus:	1. Kutsestandard “IT-turvaspetsialist, tase 5”; Infotehnoloogia ja Telekommunikatsiooni Kutsenõukogu; Otsus: 12/13.11.2018 2. Kutseharidusstandard; Vabariigi Valitsus määrus nr 130					
Õppekava õpiväljundid:	1) Teada infoturbe halduse põhialuseid 2) Rakendada protsesse, mis tagavad IKT-süsteemide turvalisuse ja osaleda nende protsesside kujundamisel ja arendamisel 3) Luua ja hoida positiivseid ärisuhteid partneritega, juurutades organisatsioonilisi protsesse ja olles kooskõlas nendega. 4) Hallata IT-süsteeme turvalisel viisil ja osaleda nende süsteemide kujundamisel ning arendamisel					
Õppekava rakendamine:	**Õppevorm** statsionaarne õpe - koolipõhine õpe **Sihtrühm** vähemalt 4. või 5. kvalifikatsioonitaseme kutset või vastavate kompetentse ja keskharidust omavad isikud					
Nõuded õpingute alustamiseks Viienda taseme jätkuõppes õpingute alustamise tingimus on vähemalt 4. või 5. kvalifikatsioonitaseme kutse või vastavate kompetentside ja keskhariduse olemasolu.						
Nõuded õpingute lõpetamiseks Õpingud viienda taseme kutseõppes loetakse lõpetatuks pärast õppekavas kirjeldatud kvalifikatsioonile vastavate õpiväljundite saavutamist. Õpiväljundite saavutatust hinnatakse kooli lõpueksamiga.						
Lõpetamisel väljastatavad dokumendid Lõputunnistus ja hinneteleht						
Õpingute läbimisel omandatav(ad)						
kvalifikatsioon(id):	IT-turvaspetsialist, tase 5					
osakutse(d):	puuduvad					
Õppekava struktuur Põhiõpingu 50 EKAP sh praktika 15 EKAP valikõpingud 10 EKAP sh lõpueksam 1,5 EKAP						
Põhiõpingute moodulid (50 EKAP)						
Õpitee ja töö muutuvas keskkonnas	5 EKAP	• ÕV1 kavandab oma õpitee, arvestades isiklikke, sotsiaalseid ja tööalaseid võimalusi ning piiranguid; • ÕV2 mõistab ühiskonna toimimist, tööandja ja organisatsiooni väljakutseid, probleeme ning võimalusi; • ÕV3 kavandab omapoolse panuse väärtuste loomisel enda ja teiste jaoks kultuurilises, sotsiaalses ja/või rahalises				

		tähenduses; • ÕV4 mõistab enda vastutust oma tööalase karjääri kujundamisel ning on motiveeritud ennast arendama;
Infoturbe haldamine	5 EKAP	• annab sisendit organisatsiooni IKT strateegia arendamisse; • rakendab organisatsiooni IKT strateegiat; • seirab/monitoorib ja võtab kasutusele meetmeid sisse tungimise, pettuse jaturvaintsidentide ning -lekete vastu; • järgib igapäevatöös parimaid praktikaid ja standardeid;
Organisatsiooni talitluspidevuse haldamine	5 EKAP	• tagab muudatuste juhtimise plaani ja tõhusa kontrolli; • minimeerib muudatustest põhjustatud teenuste katkestusi; • määratleb ja teavitab potentsiaalsetest teenustaseme katkestustest jaturvariskidest; • tagab organisatsiooni andmete ja informatsiooni turvariskide analüüsi jajuhtimise; • juhib organisatsiooni talitluspidevuse tagamise ja avariijärgse taaste plaane;
Teenuse osutamine	5 EKAP	• vastab ja dokumenteerib asjakohaselt kasutajate päringud ja teemad ninglahendab need või saadab intsidendi lahendamiseks edasi kolleegidele; • määratleb ja lahendab intsidentide algpõhjuseid; • määrab dokumenteerimise nõuded, võttes arvesse dokumentatsioonieesmärki ja rakendamise keskkonda; • kindlustab, et osapoolte vajadustest, muredest ja kaebustest on aru saadudja neile on reageeritud organisatsioonipoliitikast lähtuvalt; • jälgib töökindlusele ja jõudlusele kehtestatud nõudmiste vastavustteenustaseme lepingust (SLA) sätestatuga;
IT-lahenduste toimimise tagamine	15 EKAP	• rakendab turvalisi arvutivõrkude lahendusi; • haldab tööjaamu ja mobiiliseadmeid turvalisel viisil; • rakendab turvapoliitikat, et kindlustada serveri turvalisus; • kasutab pilvelahendusi turvaliselt; • rakendab avariijärgse taaste ja tagavarakoopia lahendusi;
IT-turvaspetsialist praktika	15 EKAP	• tutvub kooli praktikabaasis olevate praktikabaasidega, kaudseid vahendeid kasutades; • planeerib praktikajuhendi alusel isikliku praktika eesmärgid ja edastab praktikajuhendajale praktikalepingu sõlmimiseks vajalikud andmed; • paigaldab, seadistab ja halda turvelahendusi töökeskkonnas ning suhtleb klientide ja kolleegidega, järgides töös kehtestatud kvaliteednõudeid; • täidab praktikaga seonduva dokumentatsiooni vastavalt praktikakorrale;
Valikõpingute moodulid (12.5 EKAP)		
Andmebaaside turvalisus	3 EKAP	• paigaldab, seadistab ja turvab andmebaase vastavalt etteantud nõuetele.
Juniper võrguseadmed	3 EKAP	• paigaldab ja seadistab Juniper võrguseadmeid vastavalt etteantud võrgu spetsifikatsiooni nõuetele;
Skriptimine	5.5 EKAP	• loob skripte PowerShell, Bash Shell jaPhytonit kasutades vastavalt etteantud nõuetele;
Valikõpingute valimine: Õpilasel on õigus valida valikmooduleid 8,5 EKAP ulatuses antud õppekava ja/või kooli teistest		

õppekavadest või teiste õppeasutuste õppekavadest kooli õppekorralduseeskirjas sätestatud korras.	
Lõpueksami lühikirjeldus: Lõputööd ja -eksamid (1,5 EKAP) IT-turvaspetsialist lõpueksam Paigaldab, seadistab ja haldab turvalahendusi järgides töös kehtestatud kvaliteedi ja infoturbe tagamise eeskirju vastavalt etteantud juhendi alusel	
Praktika kirjeldus: Põhiõpingutest moodustab praktika 15.00 EKAPit	
Spetsialiseerumised puuduvad	
Õppekava kontaktisik	Natella Mihhailova erialade juht (IT ja multimeedia) Telefon 53479870, natella.mihhailova@ivkhk.ee
Märkused: Moodulite rakenduskava on kättesaadav: https://tahvel.edu.ee/#/curriculum/1927/version/4127	

IT-turvaspetsialist

Õppekava moodulite nimetused ja mahud(EKAP)	Maht kokku	1. õppeaasta
Põhiõpingute moodulid	**50**	**50**
Õpitee ja töö muutuvas keskkonnas	5	5
Infoturbe haldamine	5	5
Organisatsiooni talitluspidevuse haldamine	5	5
Teenuse osutamine	5	5
IT-lahenduste toimimise tagamine	15	15
IT-turvaspetsialist praktika	15	15
Valikõpingute moodulid	**8,5**	**8,5**
Juniper võrguseadmed	3	
Skriptimine	5,5	
Andmebaaside turvalisus	3	
Lõputööd ja -eksamid	**1,5**	**1,5**
IT-turvaspetsialist lõpueksam	1,5	1,5

IT-turvaspetsialist

Seosed kutsestandardi „IT turvaspetsialist“ kompetentside tegevusnäitajate ja eriala õppekava moodulite vahel.

Kompetentsi nimetus kutsestandardis	Eriala õppekava moodulid					
	Õpitee ja töö muutuvas keskkonnas	Infoturbe haldamine	Organisatsiooni talitluspidevuse haldamine	Teenuse osutamine	IT-lahenduste toimimise tagamine	IT-turvaspetsialist praktika
B.2.1 Sisendi andmine IKT rakenduse projekteerimisse/kavandamisse (e-CF A6) 1. teeb kaastööd projekteerimisel ning talitluslike tingimuste ja liideste väljatöötamisel.		x	x	x	x	
B.2.2 Tehnoloogia arengu jälgimine (e-CF A7) 1. hoiab ennast kursis IKT uuendustega, jälgides uudiskirju ja muid organisatsiooni infoturbe jaoks olulisi infokanaleid; 2. hoiab ennast kursis uute turvaohtude ja kaitsemeetoditega.	x	x	x	x	x	
B.2.3 Süsteemide integreerimine (e-CF B2) 1. teeb süsteemist varukoopia, kindlustades süsteemi tervikluse integreerimise ajal; 2. paigaldab infoturvalisust tagava riistvara, tarkvara või alamsüsteemi komponendid olemasolevasse või loodavasse süsteemi, järgidesasjakohaseid turvastandardeid ja muutuste kontrolli protseduure; 3. testib süsteemi jõudlust ja toimimist; 4. tagab süsteemi tervikluse ja koostalitluse, arvestades infoturbe aspekte (terviklus, konfidentsiaalsus, käideldavus).		x	x	x	x	x
B.2.4 Kliendile pakutava toote testimine (e-CF B3) 1. koostab, viib läbi ja hindab süstemaatilisi testimisprotseduure IKT süsteemidele (sh eelmise versiooni juurde tagasipöördumise protseduure),arvestades infoturbe nõudeid ja testimisprotsessi elutsüklit ning testimise liike; 2. annab hinnangu toote vastavuse ettevõttesisestele ja -välistele, riigisisestele ja rahvusvahelistele standarditele (sh kasutatavuse, jõudluse,töökindluse või ühilduvuse standarditele), lähtudes infoturbe aspektist; 3. koostab dokumente ja aruandeid, tõendades vajadusel vastavust sertifitseerimisnõuetele.	x	x	x	x	x	

B.2.5 Lahenduse paigaldamine (e-CF B4) 1. planeerib ja organiseerib paigaldamise ja seadistamise, arvestades juurutamise mõju olemasolevale arhitektuurile; 2. paigaldab ja seadistab süsteemi komponente (sh võrku, servereid, andmebaase, veebi- ja pilvetehnoloogiaid), lähtudes projekteerimisel võiintegreerimisel väljatöötatud juhistest; 3. kaasab täiendavaid erialaseid ressursse, nt kolmanda osapoole võrguteenuse pakkujaid; 4. kasutab võimalusel innovatiivseid lahendusi ja integreerib neid olemasolevatesse süsteemidesse ja teenustesse, arvestades turvameetmeid; 5. annab kasutajale üle täielikult töökorras lahenduse (sh dokumentatsiooni), lähtudes tarkvara pakendamise ja jaotamise meetoditest.		x	x	x	x	x
B.2.6 Dokumentatsiooni koostamine (e-CF B5) 1. koostab tooteid, teenuseid, komponente või rakendusi kirjeldavaid dokumente (sh kasutusjuhendeid ja erinevaid tehnilisi dokumente, mis onvajalikud toodete, rakenduste ja teenuste projekteerimiseks, väljatöötamiseks ja juurutamiseks), järgides asjakohaseid dokumentatsiooninõudeid ja standardeid; 2. valib dokumentide esitlemiseks sobiva stiili ja meediumi (nt esitlus, video, dokumendivormis kasutusjuhend); 3. tagab funktsionaalsuste ja omaduste nõuetekohase dokumenteerimise; 4. tagab olemasolevate dokumentide kehtivuse ja ajakohasuse; 5. kehtestab dokumenteerimisnõuded, võttes arvesse eesmärki ja keskkonda, mille suhtes seda kohaldatakse.		x	x	x	x	x
B.2.7 Kasutajatugi (e-CF C1) 1. vastab kasutaja päringutele ja küsimustele, registreerib asjakohase teabe; 2. tuvastab kasutaja probleemi(d), selgitades välja sümptomid ja küsitledes kasutajaid ning kasutades asjakohaseid IKT rakendusi; 3. otsib lahendusi kasutajate probleemidele, kasutades erinevaid andmebaase ja muid teabeallikaid; 4. lahendab kasutajate probleemid, lähtudes veaparandusprotseduuridest vajadusel saadab need lahendamiseks edasi ning optimeerib süsteemitoimivust/jõudlust kooskõlas teenusetaseme lepingutega (SLA); 5. tõlgendab süstemaatiliselt kasutaja probleeme, kasutades vajalikke töövahendeid (nt kaugtoe tööriistu, monitooringusüsteeme) ja määrateskindlaks lahendusi ning võimalikke kõrvaltoimeid; 6. jälgib lahenduse lõpptulemust ja sellest tulenevat kliendi rahulolu.	x	x	x	x	x	x
B.2.8 Muudatuste tugi (e-CF C2) 1. analüüsib ja hindab talitluslike/tehniliste muudatuste mõju süsteemile; 2. rakendab muudatusi konkreetse IKT lahenduse arendamisel, lähtudes juhistest, parimatest praktikatest, kogemusest ning infoturbeprotseduuridest; 3. koostab ja kontrollib tarkvara või riistvara muudatuste ajakava, lähtudes infosüsteemi talituslikest tingimustest ning käideldavuse nõuetest; 4. minimeerib muutustest tulenevaid teenuse katkestusi ja järgib määratletud teenusetasemelepingut; 5. kasutab funktsionaalseid ja tehnilisi lahendusi koostöös IKT meeskondadega, kes vastutavad IKT lahenduste korrashoiu ja arendamise eest; 6. haldab teabevahetust IKT meeskondadega, kes vastutavad infosüsteemide lahenduste korrashoiu ja arendamise eest; 7. muudatuste ajal tegutseb lähtuvalt äriprotsesside igapäevase toimimise vajadustest.		x	x	x	x	x

B.2.9 Teenuse osutamine (e-CF C3) 1. tagab oma pädevuse piires stabiilse ja turvalise IKT teenuse õigeaegse osutamise vastavalt kokkulepitud teenusetasemetele (SLA); 2. hindab ja rakendab ennetus- ja turvameetmeid ning kasutab monitooringusüsteeme, arvestades infoturbe ja jõudluse nõudeid; 3. jälgib kolleegide juhendamisel süsteemide talitluslikke näitajaid teenuse tõrgete ja turvaintsidentide tuvastamiseks; 4. ajakohastab teenusega seotud dokumente ja registreerib kõik olulised sündmused ja intsidendid; 5. ajakohastab ja kontrollib seire- ja haldustööriistu (nt skriptid, protseduurid); 6. analüüsib esialgset informatsiooni võimalikest teenuse taset mõjutavatest sündmustest ja tuvastatud turvariskidest ning intsidentidest jainformeerib huvitatud osapooli; 7. teeb ettepanekuid teenuse töökindluse ja turvalisus taseme parandamiseks; 8. rakendab protsesse, mis on kooskõlas asutuse IKT teenuse osutamise strateegia.	x	x	x	x	x	x
B.2.10 Probleemihaldus (e-CF C4) 1. Tuvastab turvaintsidentide algpõhjusi ja lahendab intsidente lähtudes organisatsiooni protseduuridest kasutades vajalike diagnostikatööriistu; 2. määrab kindlaks oluliste komponentide võimalikke tõrkeid ja võtab kasutusele meetmeid tõrke mõjude vähendamiseks;3. informeerib kolleege võimalikest tõrgetest; 4. suunab keerukamad juhtumid lahendamiseks edasi ning teavitab organisatsiooni kõiki tasandeid, tagamaks seisakute minimeerimiseks vajalikeressursside kasutamist ettevõttes või väljaspool; 5. teeb kindlaks, hindab ja liigitab juhtumite tüübid ning teenuse katkestused, lähtudes süsteemi taristu elementidest ja nendevahelistest seostestning tõrgete mõjust seotud äriprotsessidele; 6. registreerib juhtumid, liigitades need sümptomite ja lahenduste kaupa; 7. osaleb IKT-riskiauditi läbiviimisel.		x	x	x	x	x
B.2.11 Infoturbestrateegia väljatöötamises osaleminene (e-CF D1) 1. osaleb infoturbestrateegia väljatöötamises, lähtudes enamlevinud standarditest ja parimatest praktikatest; 2. osaleb olemasoleva olukorra kaardistamises ja annab soovitusi asjakohaste turvanõuete täitmiseks.		x	x	x	x	x
B.2.12 Personaliarendus (e-CF D9) 1. annab sisendi infoturbealase koolitusvajaduse kaardistamisel; 2. valib sobivad teenusepakkujad vajalike koolituste läbiviimiseks; 3. juhendab üksikisikuid ja meeskondi turvanõuete võimalike rikkumiste ennetamiseks ja nõustab neid olukorras, kus on tuvastatud turvanõueterikkumine.	x			x	x	
B.2.13 Riskihaldus (e-CF E3) 1. kaardistab keskkonna (sh veeb, pilv ja mobiilsed vahendid) iseloomust tulenevad riskid, tuginedes eriala parimatele praktikatele; 2. koostab ja haldab riskiregistri ja riskiohjeplaane, lähtudes parimatest praktikatest ja levinud raamistikest; 3. koordineerib riskide maandamiseks vajalikku tegevust, lähtudes koostatud plaanidest.		x	x	x	x	x

B.2.14 Infoturbe haldamine (e-CF E8) 1. osaleb ning erijuhtudel koordineerib infovarade ja nendega seotud nõrkuste kaardistamisel, nõustab ja annab sisendit infovaradeklassifitseerimisel ja nõuetekohaseks käitlemiseks; 2. osaleb infoturbe rakenduskava koostamisel, lähtudes infoturbepoliitikast; 3. registreerib infoturbeintsidendid ja jälgib nende lahendamist läbi kogu intsidendihalduse protsessi; 4. võimalusel tagab turvaintsidendi tuvastamise järgselt tõendite rikkumatuse, võimaldades turvaintsidendi edasist uurimist (nt õiguskaitseorganite,CERT, sisekontrolli poolt); 5. koostab ja haldab varundus- ja taasteplaane, lähtudes parimatest praktikatest ja levinud raamistikest;6. osaleb infoturbe auditite läbiviimisel; 7. määratleb krüpteerimise vajaduse, lähtudes organisatsioonile kehtestatud nõuetest ja ärilistest vajadustest.		x	x	x	x	x
B.2.15 IT-turvaspetsialisti kutset läbiv kompetents 1. lähtub oma töös eetilistest tõekspidamistest; 2. arvestab isiklike kutsealaste eesmärkide seadmisel organisatsiooni huve, kasutab organisatsiooni ressursse vastutustundlikult jaheaperemehelikult; 3. hindab kriitiliselt infoallikaid; 4. järgib elukestva õppe põhimõtet; 5. järgib tööprotsessi ohutusnõudeid; 6. järgib oma töös kehtestatud kvaliteedi ja infoturbe tagamise eeskirju; 7. kasutab dokumentide koostamisel ja suhtlemisel korrektset terminoloogiat; 8. suhtleb klientide ja kaastöötajatega, lähtudes heast tavast; 9. järgib valdkonnaga seotud õigusakte; 10. valdab eesti keelt tasemel B2, vene või inglise keelt tasemel B1.	x	x	x	x	x	x

X – tähistatakse, millises moodulis antud kompetentsi tegevusnäitaja omandatust hinnatakse