PÄRNUMAA KUTSEHARIDUSKESKUSE ÕPPEKAVA	
Õppekavarühm	Andmebaaside ja võrgu disain ning haldus
Õppekava nimetus	IT-turvaspetsialist
	ICT Security Specialist
Õppekava kood EHIS-es	215151

ESMAÕPPE ÕPPEKAVA					JÄTKUÕPPE ÕPPEKAVA	
EKR 2	EKR 3	EKR 4 kutsekesk-haridus	EKR 4	EKR 5	EKR 4	EKR 5
						X

Õppekava maht: 60 EKAP

Õppekava koostamise alus:
Kutsestandard "IT-Turvaspetsialist". Kinnitatud 13.11.2018. Kutsestandardi tähis 08-13112018-1.1/1k
Kutseharidusstandard, mis on vastu võetud 26.08.2013, Vabariigi Valitsuse määrus nr 130

Õppekava õpiväljundid:
Teab andmeturbega seotud põhimõisteid, tänapäeval laialt levinud turvapraktikaid ja ründevektoreid.
Analüüsib teenuseid ja organisatsiooni infrastruktuuri ning koostab ja rakendab turva- varundus- ning taasteplaane.
Administreerib ja haldab olemasolevaid teenuseid lähtudes parimates turvapraktikatest.
Monitoorib infosüsteemide tööd ja reageerib turvaintsitentidele.
Nõustab kolleege ja kliente küberturbe valdkonnas.

Õppekava rakendamine:
Õppekava rakendatakse isikule, kellel on keskharidus ning kellel on vähemalt Eesti Kvalifikatsiooniraamistiku 4.taseme IT-süsteemide nooremspetsialisti kutse või omandatud vastavad kompetentsid. Õppekava on võimalik rakendada statsionaarses õppevormis.

Nõuded õpingute alustamiseks:
Viienda taseme jätkuõppes õpingute alustamise tingimus on vähemalt 4. või 5. kvalifikatsioonitaseme IT alase esmase kutse või vastavate kompetentside ning keskhariduse olemasolu.

Nõuded õpingute lõpetamiseks:
Õpingud loetakse lõpetatuks kui õpilane on omandanud eriala õppekava moodulite õpiväljundid.
Õpiväljundite saavutatust hinnatakse lõputöö- või lõpueksamiga.

Õpingute läbimisel omandatavad kvalifikatsioonid:
Õppekava õpiväljundite omandamisel täismahus saadakse kompetentsid, mis vastavad kvalifikatsioonile "IT-turvaspetsialist", EKR tase 5

Osakvalifikatsioonid:
Puuduvad

Lõpetamisel väljastatavad dokumendid:
Viienda taseme kutseõppe lõpetanule väljastab kool lõputunnistuse koos hinnetelehega.

Õppekava struktuur
Põhiõpingute moodulid (49,5 EKAP)

Nimetus	*Maht*	*Õpiväljundid*
Küberturvalisuse alused	5,5 EKAP	tunneb küberturvalisusega seotud põhimõisteid ning modernseid parimaid turvapraktikaid nimetab tänapäeval kõige rohkem levinud ründevektoreid sooritab infosüsteemidele riskianalüüsi lähtudes parimatest praktikatest analüüsib rünnete poolt kahjustatud süsteeme ning koostab intsidendiraporte
Veebirakenduste turvalisus	5 EKAP	suhtleb kliendiga ning nõustab teda veebiturvalisuse valdkonnas dokumenteerib ja eemaldab kliendi veebiteenustes esinevad turvaprobleemid seadistab veebiservereid ja veebipõhiseid tulemüüre lähtuvalt parimatest turvapraktikatest
IT õigus ja eetika	4 EKAP	teab eestis ja euroopas laialt levinud andmekaitse seaduseid ning turvastandardeid oskab tagada isikuandmete kaitse ja autoriõigused rakendab igapäeva töös valdkonna parimaid praktikaid ja lähtub kutse-eetika väärtustest
Arvutivõrkude turvalisus	5 EKAP	mõistab arvutivõrkudest tulenevaid ohte

		tagab arvutivõrkude turvalisuse erinevates võrguseadmetes seab üles ning haldab ründetuvastus- ja ennetussüsteeme
Võrguteenuste turvalisus	4 EKAP	mõistab peamistest võrguteenustest tulenevaid ohte tagab võrguteenuste turvalise ja efektiivse töö seab üles ning haldab logimis- ja raporteerimissüsteeme
Organisatsiooni taristu turvalisus ja haldus	7 EKAP	tagab uute lahenduste integreerimise olemasolevasse süsteemi ilma infosüsteemis katkestusi tekitamata koostab organisatsiooni kriitiliste süsteemide varundus- ,uuendus ning taasteplaane ja tagab nende rakendamise seadistab monitooringu teenuseid intsidentide tuvastamiseks ja nendele reageerimiseks kasutab erinevates operatsioonisüsteemides laialt levinud turvateenuseid organisatsiooni turvalisuse tagamiseks kaardistab organisatsiooni taristut ning osaleb infoturbe strateegia väljatöötamises
Praktika	15 EKAP	suhtleb organisatsioonis olevate inimestega või klientidega ning nõustab ja koolitab neid infoturbe valdkonnas tagab olemasolevate teenuste turvalise ja efektiivse töö loob taaste- ja varundusplaane ning tagab nende rakendamise organisatsioonis viib läbi uute lahenduste integratsiooni olemasolevasse infrastruktuuri tagades võimalikult väikese teenuste katkestusaja lähtub oma töös õiguslikest ettekirjutustest, eetikareeglitest ja valdkonna parimatest praktikatest
Operatsioonisüsteemid	4 EKAP	haldab operatsioonisüsteeme lähtudes pariamtest turvapraktikatest loob turvapoliitikaid ja tagab nende rakendamise operatsioonisüsteemide taasteplaani loomine ja selle kasutamise juurutamine

Põhiõpingute moodulid 49.5 EKAP, millest 15 EKAP on ettevõttepraktika.
Valikõpingute moodulid 9 EKAP.
Lõputööd ja -eksamid 1.5 EKAP.

Valikõpingute moodulid (9 EKAP)

Nimetus	*Maht*	*Õpiväljundid*
Sissejuhatus programmeerimisse	4 EKAP	teab programmeerimiseks vajalikul tasemel python keelega seotud põhimõisteid ja konstruktsioone kirjutab lihtsamaid programme kasutades funktsioone, tsu□kleid ja tingimuslauseid kasutab keerulisemaid andmestruktuure ja faile rakenduste loomisel automatiseerib süsteemide administreerimisel aset leidvaid haldustegevusi
Konteiner lahenduste haldus	5 EKAP	saab aru konteinerite tööpõhimõtetest ning oskab nimetada erinevaid rakendusvaldkondi loob ja haldab konteinereid kasutades tarkvaralist lahendust Docker kasutab konteinerite haldusvahendit Kubernetes konteinerite kasutuselevõtu, levitamise ja skaleeritavuse automatiseerimiseks
Palo Alto võrguseadmete haldus	5 EKAP	tunneb Palo Alto tootevalikut ja neis kasutatavat tarkvara seab üles ning seadistab arvutivõrgu ja selle tugiteenused tagab arvutivõrkude turvalisuse kasutades Palo Alto tulemüürides leiduvaid lahendusi

Valikõpingute valimise võimalused:
Valikõpingu moodulid on koostatud, et toetada antud õppekava käigus omandatavaid oskuseid. Valikõpingud annavad ka õpilastele võimaluse spetsialiseeruda täpsemalt enda soovitud suundades.

Kool avab valikõpingutena spetsialiseerumise, kui selle spetsialiseerumise soovijaid on vähemalt 50% õppijatest.

Õpilasel on võimalik valida 9 EKAP ulatuses järgmiste moodulite hulgast:
Sissejuhatus programmeerimisse 4 EKAP
Palo Alto võrguseadmete haldus 5 EKAP
Konteiner lahenduste haldus 5 EKAP

Samuti on õpilasel õigus valida valikmooduleid kooli teistest õppekavadest või teiste õppeasutuste õppekavadest kooli õppekorralduseeskirjas sätestatud korras.

Lõputööd ja -eksamid (1,5 EKAP)

IT-turvaspetsialisti lõpueksam	1,5 EKAP	paigaldab, haldab ning turvab etteantud infosüsteemi ja seal olevaid tarkvaralisi lahendusi lähtudes töös etteantud juhendist. Lähtub parimatest turvapraktikatest, seaduslikest nõuetest ja turvaraamistikest ning dokumenteerib oma töö vastavalt nõuetele kasutades korrektset erialast terminoloogiat

Praktika:

Põhiõpingutest moodustab praktika 15.00 EKAPit.

Õppekava kontaktisik:

Kristjan Leotoots
kutseõpetaja
Telefon , kristjan.leotoots@hariduskeskus.ee

Märkused:

Kooli õppekava ja moodulite rakenduskavad on kättesaadavad:
https://ois.hariduskeskus.ee/veebivormid/oppekavad/oppekava_pdf?oppekava=453
https://ois.hariduskeskus.ee/veebivormid/oppekavad/oppekava_pdf?oppekava=453&rakenduskavad=jah (koos moodulite rakenduskavadega)

IT-turvaspetsialist

Õppekava moodulite nimetused ja mahud(EKAP)	Maht kokku	1. õppeaasta
Põhiõpingute moodulid	**49,5**	**49,5**
Küberturvalisuse alused	5,5	5,5
Veebirakenduste turvalisus	5	5
IT õigus ja eetika	4	4
Arvutivõrkude turvalisus	5	5
Võrguteenuste turvalisus	4	4
Organisatsiooni taristu turvalisus ja haldus	7	7
Praktika	15	15
Operatsioonisüsteemid	4	4
Valikõpingute moodulid	**9**	**9**
Sissejuhatus programmeerimisse	4	
Konteiner lahenduste haldus	5	
Palo Alto võrguseadmete haldus	5	
Lõputööd ja -eksamid	**1,5**	**1,5**
IT-turvaspetsialisti lõpueksam	1,5	1,5

IT-turvaspetsialist

Seosed kutsestandardi „IT-turvaspetsialist, tase 5“ kompetentside tegevusnäitajate ja eriala õppekava moodulite vahel.

Kompetentsi nimetus kutsestandardis	Eriala õppekava moodulid							
	Küberturvalisuse alused	Veebirakenduste turvalisus	IT õigus ja eetika	Arvutivõrkude turvalisus	Võrguteenuste turvalisus	Organisatsiooni taristu turvalisus ja haldus	Praktika	Operatsioonisüsteemid
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	X	X	X	X	X	X	X	
2. hoiab ennast kursis uute turvaohtude ja kaitsemeetoditega	X	X		X	X	X	X	X
B.2.3 Süsteemide integreerimine (e-CF B2)								
1. teeb süsteemist varukoopia, kindlustades süsteemi tervikluse integreerimise ajal		X				X	X	X
2. paigaldab infoturvalisust tagava riistvara, tarkvara või alamsüsteemi komponendid olemasolevasse või loodavasse süsteemi, järgides asjakohaseid turvastandardeid ja muutuste kontrolli protseduure		X		X		X	X	X
3. testib süsteemi jõudlust ja toimimist		X		X	X	X	X	
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		X				X	X	
2. annab hinnangu toote vastavuse ettevõttesisestele ja -välistele, riigisisestele ja rahvusvahelistele standarditele (sh kasutatavuse,	X		X			X	X	

jõudluse, töökindluse või ühilduvuse standarditele), lähtudes infoturbe aspektist								
3. koostab dokumente ja aruandeid, tõendades vajadusel vastavust sertifitseerimisnõuetele	X		X			X	X	
B.2.5 Lahenduse paigaldamine (e-CF B4)								
1. planeerib ja organiseerib paigaldamise ja seadistamise, arvestades juurutamise mõju olemasolevale arhitektuurile	X					X	X	
2. paigaldab ja seadistab süsteemi komponente (sh võrku, servereid, andmebaase, veebi- ja pilvetehnoloogiaid), lähtudes projekteerimisel või integreerimisel väljatöötatud juhistest	X	X		X	X	X	X	X
3. kaasab täiendavaid erialaseid ressursse, nt kolmanda osapoole võrguteenuse pakkujaid	X	X			X	X	X	
4. kasutab võimalusel innovatiivseid lahendusi ja integreerib neid olemasolevatesse süsteemidesse ja teenustesse, arvestades turvameetmeid		X		X	X	X	X	
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 on vajalikud toodete, rakenduste ja teenuste projekteerimiseks, väljatöötamiseks ja juurutamiseks), järgides asjakohaseid dokumentatsiooninõudeid ja standardeid	X	X		X	X	X	X	X
2. valib dokumentide esitlemiseks sobiva stiili ja meediumi (nt esitlus, video, dokumendivormis kasutusjuhend)	X	X	X	X	X	X	X	X
3. tagab funktsionaalsuste ja omaduste nõuetekohase dokumenteerimise	X	X		X	X	X	X	X
4. tagab olemasolevate dokumentide kehtivuse ja ajakohasuse;	X	X	X	X	X	X	X	X
5. kehtestab dokumenteerimisnõuded, võttes arvesse eesmärki ja keskkonda, mille suhtes seda kohaldatakse	X	X	X			X	X	
B2.7 Kasutajatugi (e-CF C1)								
1. vastab kasutaja päringutele ja küsimustele, registreerib asjakohase teabe	X		X			X	X	
2. tuvastab kasutaja probleemi(d), selgitades välja sümptomid ja küsitledes kasutajaid ning kasutades asjakohaseid IKT rakendusi	X		X			X	X	
3. otsib lahendusi kasutajate probleemidele, kasutades erinevaid andmebaase ja muid teabeallikaid	X					X	X	
4. lahendab kasutajate probleemid, lähtudes veaparandusprotseduuridest vajadusel saadab need lahendamiseks edasi ning optimeerib süsteemi toimivust/jõudlust kooskõlas teenusetaseme lepingutega (SLA)	X					X	X	
5. tõlgendab süstemaatiliselt kasutaja probleeme, kasutades vajalikke töövahendeid (nt kaugtoe tööriistu, monitooringusüsteeme) ja määrates kindlaks lahendusi ning võimalikke kõrvaltoimeid	X					X	X	
6. jälgib lahenduse lõpptulemust ja sellest tulenevat kliendi rahulolu						X	X	
B2.8. Muudatuste tugi (e-CF C2)								
1. analüüsib ja hindab talitluslike/tehniliste muudatuste mõju süsteemile		X		X	X	X	X	X
2. rakendab muudatusi konkreetse IKT lahenduse arendamisel, lähtudes juhistest, parimatest praktikatest, kogemusest ning infoturbe protseduuridest		X		X	X	X	X	X
3. koostab ja kontrollib tarkvara või riistvara muudatuste ajakava, lähtudes infosüsteemi talituslikest tingimustest ning käideldavuse nõuetest		X				X	X	X
4. minimeerib muutustest tulenevaid teenuse katkestusi ja järgib määratletud teenusetasemelepingut		X				X	X	

5. kasutab funktsionaalseid ja tehnilisi lahendusi koostöös IKT meeskondadega, kes vastutavad IKT lahenduste korrashoiu ja arendamise eest		X		X	X	X	X	
6. haldab teabevahetust IKT meeskondadega, kes vastutavad infosüsteemide lahenduste korrashoiu ja arendamise eest		X		X	X	X	X	
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)		X	X			X	X	
2. hindab ja rakendab ennetus- ja turvameetmeid ning kasutab monitooringusüsteeme, arvestades infoturbe ja jõudluse nõudeid	X	X		X	X	X	X	
3. jälgib kolleegide juhendamisel süsteemide talitluslikke näitajaid teenuse tõrgete ja turvaintsidentide tuvastamiseks		X		X	X	X	X	
4. ajakohastab teenusega seotud dokumente ja registreerib kõik olulised sündmused ja intsidendid	X	X	X	X	X	X	X	X
5. ajakohastab ja kontrollib seire- ja haldustööriistu (nt skriptid, protseduurid)		X		X	X	X	X	X
6. analüüsib esialgset informatsiooni võimalikest teenuse taset mõjutavatest sündmustest ja tuvastatud turvariskidest ning intsidentidest ja informeerib huvitatud osapooli	X	X	X	X	X	X	X	X
7. teeb ettepanekuid teenuse töökindluse ja turvalisus taseme parandamiseks	X	X	X			X	X	
8. rakendab protsesse, mis on kooskõlas asutuse IKT teenuse osutamise strateegia	X	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	X	X		X	X	X	X	X
2. määrab kindlaks oluliste komponentide võimalikke tõrkeid ja võtab kasutusele meetmeid tõrke mõjude vähendamiseks	X	X		X	X	X	X	X
3. informeerib kolleege võimalikest tõrgetest	X	X				X	X	
4. suunab keerukamad juhtumid lahendamiseks edasi ning teavitab organisatsiooni kõiki tasandeid, tagamaks seisakute minimeerimiseks vajalike ressursside kasutamist ettevõttes või väljaspool	X	X	X			X	X	
5. teeb kindlaks, hindab ja liigitab juhtumite tüübid ning teenuse katkestused, lähtudes süsteemi taristu elementidest ja nendevahelistest seostest ning tõrgete mõjust seotud äriprotsessidele	X	X		X	X	X	X	
6. registreerib juhtumid, liigitades need sümptomite ja lahenduste kaupa	X	X		X	X	X	X	
7. osaleb IKT-riskiauditi läbiviimisel	X		X			X	X	
B.2.11 Infoturbestrateegia väljatöötamises osaleminene (e-CF D1)								
1. osaleb infoturbestrateegia väljatöötamises, lähtudes enamlevinud standarditest ja parimatest praktikatest	X		X			X	X	
2. osaleb olemasoleva olukorra kaardistamises ja annab soovitusi asjakohaste turvanõuete täitmiseks	X		X			X	X	
B.2.12 Personaliarendus (e-CF D9)								
1. annab sisendi infoturbealase koolitusvajaduse kaardistamisel	X		X			X	X	
2. valib sobivad teenusepakkujad vajalike koolituste läbiviimiseks	X		X			X	X	
3. juhendab üksikisikuid ja meeskondi turvanõuete võimalike rikkumiste ennetamiseks ja nõustab neid olukorras, kus on tuvastatud	X		X			X	X	

turvanõuete rikkumine								
B.2.13 Riskihaldus (e-CF E3)								
1. kaardistab keskkonna (sh veeb, pilv ja mobiilsed vahendid) iseloomust tulenevad riskid, tuginedes eriala parimatele praktikatele	X	X		X	X	X	X	X
2. koostab ja haldab riskiregistri ja riskiohjeplaane, lähtudes parimatest praktikatest ja levinud raamistikest	X	X	X			X	X	X
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 infovarade klassifitseerimisel ja nõuetekohaseks käitlemiseks	X	X		X	X	X	X	X
2. osaleb infoturbe rakenduskava koostamisel, lähtudes infoturbepoliitikast	X					X	X	
3. registreerib infoturbeintsidendid ja jälgib nende lahendamist läbi kogu intsidendihalduse protsessi	X					X	X	
4. võimalusel tagab turvaintsidendi tuvastamise järgselt tõendite rikkumatuse, võimaldades turvaintsidendi edasist uurimist (nt õiguskaitseorganite, CERT, sisekontrolli poolt)	X		X			X	X	
5. koostab ja haldab varundus- ja taasteplaane, lähtudes parimatest praktikatest ja levinud raamistikest	X	X				X	X	X
6. osaleb infoturbe auditite läbiviimisel	X	X	X			X	X	
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	X	X	X	X	X	X	X	X
2. arvestab isiklike kutsealaste eesmärkide seadmisel organisatsiooni huve, kasutab organisatsiooni ressursse vastutustundlikult ja heaperemehelikult	X	X	X	X	X	X	X	X
3. hindab kriitiliselt infoallikaid	X	X	X	X	X	X	X	X
4. järgib elukestva õppe põhimõtet	X	X	X	X	X	X	X	X
5. järgib tööprotsessi ohutusnõudeid	X	X	X	X	X	X	X	X
6. järgib oma töös kehtestatud kvaliteedi ja infoturbe tagamise eeskirju	X	X	X	X	X	X	X	X
7. kasutab dokumentide koostamisel ja suhtlemisel korrektset terminoloogiat	X	X	X	X	X	X	X	X
8. suhtleb klientide ja kaastöötajatega, lähtudes heast tavast	X	X	X	X	X	X	X	X
9. järgib valdkonnaga seotud õigusakte	X	X	X	X	X	X	X	X
10. valdab eesti keelt tasemel B2, vene või inglise keelt tasemel B1	X	X	X	X	X	X	X	X

X – tähistatakse, millises moodulis antud kompetentsi tegevusnäitaja omandatust hinnatakse

Võrdlusanalüüsi koostaja **Kristjan Leotoots, kutseõpetaja**