RTU studiju kurss "Kibedrošības arhitektūra"

33000 Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte

Vispārējā informācija

Kods	DE1040
Nosaukums	Kibedrošības arhitektūra
Studiju kursa statuss programmā	Brīvās izvēles
Atbildīgais mācībspēks	Mārtiņš Bonders - Docents (praktiskais)
Mācībspēks	Rūta Pirta - Doktors, Docents
Apjoms daļās un kredītpunktos	1 daļa, 5.0 kredītpunkti
Studiju kursa īstenošanas valodas	LV
Anotācija	Mūsdienās kiberdrošības arhitektūra kļūst par vienu no kritiski svarīgākajiem informācijas tehnoloģiju nozares virzieniem, jo organizācijas saskaras ar arvien sarežģītākiem kiberdraudiem. Kiberdrošības arhitektūra aptver vislabākās prakses ieteikumus, kas nodrošina strukturētu pieeju drošu IT sistēmu projektēšanai, ieviešanai un pārvaldībai. Šīs prakses ietver risku pārvaldību, tīklu un lietojumprogrammu drošības nodrošināšanu, datu aizsardzību un kriptogrāfijas risinājumu integrēšanu. Kiberdrošības arhitektūras pielietojums palīdz organizācijām standartizēt drošības pasākumus, optimizēt IT resursu pārvaldību un nodrošināt biznesa nepārtrauktību, pat saskaroties ar ārējiem un iekšējiem apdraudējumiem. Studiju kurss sniedz teorētisku un praktisku ieskatu kiberdrošības arhitektūras izstrādes procesā un pieejamo praktisko rīku un sistēmu apskatu. Tas dod priekštatu, kā izveidot un nepārtraukti uzlabot arhitektūras modeļus, izstrādāt atbilstošu arhitektūras dokumentāciju un specifikācijas, kā arī koordinēt kiberdrošības komponentu drošu izstrādi, integrāciju un uzturēšanu saskaņā ar standartiem un citām saistītām prasībām. Studiju kursā tiek aplūkoti industrijā populāri un jauni risinājumi, kas atbalsta drošas IT infrastruktūras ieviešanu, sākot no “DevSecOps” principu integrēšanu programmatūras izstrādē līdz mākslīgā intelekta izmantošanai kiberdraudu analīzē. Tā ietvaros studenti apgūs prasmes drošības rīku ieviešanā, lietošanā, infrastruktūras testēšanā, esošās infrastruktūras audita procesa nodrošināšanā un ilgtermiņa kiberdrošības stratēģijas plānošanā. Studiju kurss ir pielāgots kombinēto studiju metodikai, ietverot gan asinhronas, gan sinhronas studiju aktivitātes. Beidzot studiju kursu, studenti būs sagatavoti pielietot iegūtās zināšanas gan praktiskā, gan akadēmiskā vidē, kā arī turpināt profesionālo izaugsmi kiberdrošības arhitektūra izstrādē un ieviešanā. Studiju kurss sniedz nepieciešamās zināšanas ENISA lomai "Kiberdrošības arhitektūras speciālists".
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Studiju kura mērķis ir veidot prasmes un sagatavot studentus profesionālai darbībai kiberdrošības arhitektūras jomā, nodrošinot teorētiskas zināšanas un praktiskas prasmes, kas nepieciešamas, lai izstrādātu, ieviestu un uzturētu drošu, ilgtspējīgu un efektīvu IT infrastruktūru, vienlaikus atbalstot organizācijas biznesa mērķus un riska pārvaldības stratēģijas. Studiju kursa uzdevumi: - radīt izpratni par kiberdrošības arhitektūras pielietošanu, lai nodrošinātu organizācijas IT sistēmu ilgtermiņa noturību un aizsardzību pret draudiem; - sniegt zināšanas par starptautiskajiem drošības standartiem; - veidot prasmi plānot un ieviest drošības risinājumus tīkla un lietojumprogrammu līmenī; - veidot spēju prognozēt tehnoloģiju, draudu attīstību un pielāgot organizācijas drošības arhitektūru jauniem apdraudējumiem; - veidot izpratni par komunikācijas nozīmīgumu, lai pārliecinātu organizācijas vadību par drošības uzlabošanas nepieciešamību un kiberdrošības ieviešanas ieguvumiem; - attīstīt spēju ieviest un pielietot mūsdienu drošības rīkus, piemēram, IDS/IPS, VPN, ugunsmūri, žurnālfailu pārvaldību un šifrēšanas tehnoloģijas, drošas IT infrastruktūras arhitektūras izveidē; - iemācīt sagatavot arhitektūras dokumentāciju un specifikācijas; - veidot spēju izstrādāt sistēmas un arhitektūras, pamatojoties uz iekļautiem drošības un privātuma kiberdrošības principiem (“security and privacy by design”).
Patstāvīgais darbs, tā organizācija un uzdevumi	Patstāvīgais darbs tiek plānots, lai studenti padziļinātu kursā apgūto materiālu un attīstītu praktiskās iemaņas. Tajā tik iekļauta literatūras izpēte, tehnoloģiju pielietošana, projekta izstrāde. Individuālais darbs: studenti pilda uzdevumus patstāvīgi, izmantojot kursa materiālus un norādītās tehnoloģijas. Grupu darbs: studenti tiek sadalīti grupās, lai veidotu komandu un realizētu izmeklēšanas uzdevumu.

Literatūra	Obligātā/Obligatory: 1. Cyber Security Basics: Protect your organization by applying the fundamentals. Author: Don Franke. Publisher: CreateSpace Independent Publishing Platform, 2016. ISBN: 978-1522952190. 2. Industrial cybersecurity: efficiently secure critical infrastructure systems. Author: Pascal Ackerman. Publisher: Packt Publishing Ltd, 2017. ISBN: 978-1788395984 3. Introduction to computer networks and cybersecurity. Author: Chwan-Hwa (John) Wu, Auburn University, J. David Irwin. Publisher: CRC Press; 1st edition, 2013. ISBN: 978-1466572133 4. Kali Linux - Assuring Security by Penetration Testing: Master the Art of Penetration Testing with Kali Linux. Author:Lee Allen, Tedi Heriyanto, Shakeel Ali. Publisher: Packt Pub Ltd; 2nd ed. edition, 2014. ISBN: 978-1849519489 5. Information Security: Principles and Practice. Author: Mark Stamp. Publisher: Wiley; 2nd edition, 2011. ISBN: 978-0470626399 Papildu/Additional: 1. Essential Cybersecurity Science: build, test, and evaluate secure systems. Author: Josiah Dykstra. Publisher: O'Reilly Media; 1st edition, 2016. ISBN: 978-1491920947
Nepieciešamās priekšzināšanas	Izpratne par datortīkla uzbūvi un dažāda veida operētājsistēmu darbību. Pamata zināšanu līmenis darbā ar Linux operētājsistēmu un izpratne par hipervizoru pielietošanas iespējām.

Studiju kursa saturs

Saturs	Pilna un nepilna laika klātienes studijas		Nepilna laika neklātienes studijas	
	Kontakt stundas	Patstāv. darbs	Kontakt stundas	Patstāv. darbs
Kiberdrošības arhitektūras nozīme, mūsdienu kiberdrošības izaicinājumi un to ietekme uz IT sistēmām. Kiberdrošības ieteikumi un labā prakse. Kiberdrošības standarti, metodoloģija un ietvari.	8	7	0	0
Mākslīgā intelekta pielietojums kiberdrošības arhitektūras izstrādē un ieviešanā. Sistēmu, pakalpojumu un produktu izstrādes cikls.	6	6	0	0
Drošības arhitektūras pamatelementi, drošības kontroles un tehnoloģijas, lietojumprogrammu un tīklu segmentācija. Pieejamie rīki un risinājumi.	8	6	0	0
Kiberdrošības risku pārvaldība, analīze, atbilstība dažādām prasībām, drošības politikas izstrāde. Pieejamie rīki un risinājumi. Konfidencialitātes jeb privātumu uzlabojošas tehnoloģijas (PET).	8	6	0	0
Lietojumprogrammu un tīkla drošības principi, lietojumprogrammu un tīkla iekārtu ievainojamības, to pārvaldība, drošības prasību ieviešana un kontrole. Pieejamie rīki un risinājumi.	8	6	0	0
Drošas datu pārraides arhitektūras izstrāde un tehniskie risinājumi, datortīkla draudi, kiberuzbrukumi un to novēršana. Pieejamie rīki un risinājumi.	5	8	0	0
Operacionālā drošība un kiberdrošības arhitektūras uzraudzība, Zero Trust arhitektūras princips.	5	6	0	0
Datu drošība un šifrēšanas metodes, rezerves kopiju veidošanas stratēģija. Pieejamie rīki un risinājumi.	6	6	0	0
Incidentu pārvaldība un reaģēšana, incidentu pārvaldības process, incidentu atklāšana un analīze, incidentu pārvaldības rīki un tehnoloģijas. Kiberdrošības prasību ziņojuma izveidošana.	6	6	0	0
Mākoņdatošanas un lokālo hipervizoru drošība, drošības izaicinājumi un piekļuves aizsardzības, kontroles veidi.	6	6	0	0
Drošības un veiktspējas prasību nozīme IT iepirkumos, tai skaitā nefunkcionālo prasību definēšana kiberdrošības iepirkumos.	2	2	0	0
Kopā:	68	65	0	0

Sasniedzamie studiju rezultāti un to vērtēšana

Sasniedzamie studiju rezultāti	Rezultātu vērtēšanas metodes
Spēj identificēt un analizēt mūsdienu kiberdrošības izaicinājumus un to ietekmi uz IT sistēmām, kā arī izvērtēt kiberdrošības arhitektūras nozīmi organizācijas stratēģiskajā attīstībā.	Izpildīti praktiskie uzdevumi. Tests par atbilstošajām tēmām. Tests iekļaus jautājumus no teorētiskās un praktiskās daļas. // Lai veiksmīgi nokārtotu testu, ir jāatbild pareizi uz vismaz 70% jautājumu. Lai praktiskie uzdevumi tiktu ieskaitīti, jābūt iesniegtai uzdevuma izpildes atskaitei ar izpildītiem visiem uzdevuma nosacījumiem.
Spēj izveidot un ieviest drošības arhitektūras risinājumus, izmantojot mākslīgā intelekta un automatizācijas tehnoloģijas, lai efektīvi novērstu kiberdraudus.	Izpildīti praktiskie uzdevumi. Tests par atbilstošajām tēmām. Tests iekļaus jautājumus no teorētiskās un praktiskās daļas. // Lai veiksmīgi nokārtotu testu, ir jāatbild pareizi uz vismaz 70% jautājumu. Lai praktiskie uzdevumi tiktu ieskaitīti, jābūt iesniegtai uzdevuma izpildes atskaitei ar izpildītiem visiem uzdevuma nosacījumiem.
Spēj konsultēt jautājumos, kas saistīti ar kiberdrošības arhitektūras ieviešanu un pārvaldību.	Grupu darbs, eksāmens (zināšanu pārbaudes testa formā). Tests iekļaus jautājumus no teorētiskās un praktiskās daļas. // Lai veiksmīgi nokārtotu testu, ir jāatbild pareizi uz vismaz 70% jautājumu. Lai veiksmīgi nokārtotu grupu darbu ir jāizpilda visi grupu darba izpildes nosacījumi un jāprezentē darba saturu.

Izprot drošības arhitektūras pamatelementus, drošības kontroles un tehnoloģijas, kā arī tīkla un lietojumprogrammu segmentācijas principus, lai izveidotu integrētus drošības risinājumus.	Izpildīti praktiskie uzdevumi. Tests par atbilstošajām tēmām. Tests iekļaus jautājumus no teorētiskās un praktiskās daļas. // Lai veiksmīgi nokārtotu testu, ir jāatbild pareizi uz vismaz 70% jautājumu. Lai praktiskie uzdevumi tiktu ieskaitīti, jābūt iesniegtai uzdevuma izpildes atskaitei ar izpildītiem visiem uzdevuma nosacījumiem.
Spēj nodrošināt mākoņdatošanas un lokālo hipervizoru drošību, identificējot piekļuves aizsardzības un kontroles metodes, lai risinātu drošības izaicinājumus.	Izpildīti praktiskie uzdevumi. Tests par atbilstošajām tēmām. Tests iekļaus jautājumus no teorētiskās un praktiskās daļas. // Lai veiksmīgi nokārtotu testu, ir jāatbild pareizi uz vismaz 70% jautājumu. Lai praktiskie uzdevumi tiktu ieskaitīti, jābūt iesniegtai uzdevuma izpildes atskaitei ar izpildītiem visiem uzdevuma nosacījumiem.
Izprot kiberdrošības komponentu izstrādi, integrāciju un uzturēšanu, nodrošinot kiberdrošības specifikācijas.	Izpildīti praktiskie uzdevumi. // Lai praktiskie uzdevumi tiktu ieskaitīti, jābūt iesniegtai uzdevuma izpildes atskaitei ar izpildītiem visiem uzdevuma nosacījumiem.
Spēj risināt kiberdrošības incidentus, pārvaldīt incidentu identificēšanu un analīzi, kā arī pielietot efektīvus incidentu pārvaldības rīkus un tehnoloģijas.	Izpildīti praktiskie uzdevumi. Tests par atbilstošajām tēmām. Tests iekļaus jautājumus no teorētiskās un praktiskās daļas. Grupu darbs. // Lai veiksmīgi nokārtotu testu, ir jāatbild pareizi uz vismaz 70% jautājumu. Lai praktiskie uzdevumi tiktu ieskaitīti, jābūt iesniegtai uzdevuma izpildes atskaitei ar izpildītiem visiem uzdevuma nosacījumiem. Lai veiksmīgi nokārtotu grupu darbu ir jāizpilda visi grupu darba izpildes nosacījumi un jāprezentē darba saturu.

Studiju rezultātu vērtēšanas kritēriji

Kritērijs	% no kopējā vērtējuma
Teorētisko zināšanu pārbaude (tests, grupu darbs)	20
Praktisko uzdevumu izpilde	30
Kursa noslēguma pārskata izveide	20
Eksāmens	30
Kopā:	100

Studiju kursa plānojums

Daļa	KP	Stundas			Pārbaudījumi			Brīvās izvēles pārbaudījumi		
		Lekcijas	Prakt d.	Laborat	Ieskaite	Eksām.	Darbs	Ieskaite	Eksām.	Darbs
1.	5.0	34.0	34.0	0.0		*				