RTU studiju kurss "Digitālā izmeklēšana"

33000 Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte

Vispārējā informācija

Kods	DE1039
Nosaukums	Digitālā izmeklēšana
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	Studiju kurss ir veidots, lai studentiem sniegtu visaptverošu izpratni par digitālās izmeklēšanas procesiem un to pielietojumu mūsdienu kiberincidentu pārvaldībā. Studiju kurss ietver galvenos digitālās izmeklēšanas aspektus, sākot no pierādījumu iegūšanas un analīzes līdz incidentu dokumentēšanai un risinājumu ieviešanai. Tas balstās uz starptautiski atzītām metodoloģijām, piemēram, NIST un SANS, lai nodrošinātu sistemātisku pieeju kiberapdraudējumu identificēšanai un novēršanai. Studenti apgūs gan teorētisko bāzi par tīkla un resursdatoru datu vākšanu un analīzi, gan attīstīs praktiskās iemaņas, strādājot ar dažādiem rīkiem. Studiju kursa ietvaros tiks apskatīti būtiski temati, piemēram, tīkla un resursdatoru pierādījumu iegūšana, digitālās izmeklēšanas juridiskie aspekti, uzbrukumu izmeklēšana un incidentu pārvaldība, izmantojot kiberdrošības modeļus. Studenti tiks iesaistīti reālistiskās situācijās, lai simulētu un analizētu dažādu incidentu izmeklēšanas procesu no sākuma līdz beigām, veidojot strukturētus incidentu pārskatus un sniedzot praktiskas rekomendācijas organizācijas drošības uzlabošanai. Studiju kurss ir īpaši vērsts uz to, lai studentiem attīstītu spējas efektīvi risināt sarežģītas problēmas, vadīt izmeklēšanas procesu un pielietot proaktīvas pieejas, lai identificētu un novērstu potenciālos draudus. Tiek uzsvērta spēja darboties komandā un prezentēt rezultātus tehniskai komandai un uzņēmuma vadībai. Beidzot studiju kursu, studenti būs sagatavoti pielietot iegūtās zināšanas gan praktiskā, gan akadēmiskā vidē, kā arī turpināt profesionālo izaugsmi kiberdrošības un digitālās izmeklēšanas jomā. Studiju kurss ir pielāgots kombinēto studiju metodikai, ietverot gan asinhronas, gan sinhronas studiju aktivitātes. Studiju kurss sniedz nepieciešamās zināšanas ENISA lomai "Digitālās izmeklēšanas (kriminālistikas) speciālists".
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Studiju kursa mērķis ir veidot studentiem prasmes, izpratni un kompetences kiberincidentu identificēšanā, analīzē, un efektīvā risināšanā, izmantojot digitālās izmeklēšanas principus un tehnoloģijas. Studiju kursa uzdevumi: - radīt izpratni par digitālās izmeklēšanas lomu un tās pielietojumu incidentu fiksēšanā; - veidot prasmes juridisku un tehnisku aspektu digitālo pierādījumu vākšanā un izmantošanā; - iemācīt identificēt, vākt un analizēt tīkla un resursdatoru pierādījumus, izmantojot atbilstošus rīkus un metodoloģijas; - iemācīt strukturēt incidentu pārskatus un pamatot rekomendācijas turpmākiem drošības pasākumiem; - veidot prasmes proaktīvi analizēt un atklāt potenciālus draudus, izmantojot digitālās izmeklēšanas un incidentu pārvaldības metodes; - radīt izpratni par digitālo izmeklēšanu, koordinējot komandas darbu un komunikāciju ar ieinteresētajām pusēm; - veidot spēju identificēt, atgūt, dokumentēt un analizēt digitālos pierādījumus; - veidot prasmes sistemātiski un deterministiski dokumentēt, ziņot un iepazīstināt ar digitālās kriminālistikas analīzes konstatējumiem un rezultātiem.
Patstāvīgais darbs, tā organizācija un uzdevumi	Patstāvīgais darbs tiek plānots, lai studenti padziļinātu studiju kursā apgūto materiālu un attīstītu praktiskās iemaņas. Tajā tiek 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. Guide to computer forensics and investigations. Author: Bill Nelson, Amelia Phillips, Chris Steuart. Publisher: Cengage Learning, 2018. ISBN: 978-1337568944 2. Digital Forensics Explained. Author: Greg Gogolin. Publisher: Auerbach Publications; 1st edition, 2012. ISBN: 978-1439874950 3. Computer Forensics JumpStart. Author: Diane Barrett, Neil Broom, K. Rudolph, Michael G. Solomon, Ed Tittel. Publisher: John Wiley & Sons INC International Concepts, 2011. ISBN: 9780470931660 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. Computer Forensics For Dummies. Author: L.Volonino, R.Anzaldua. Publisher: For Dummies; 1st edition, 2011. ISBN: 978-0470371916

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
Ievads kiberdrošībā, digitālajā izmeklēšanā un kiberdrošības incidentu pārvaldībā.	8	8	0	0
Digitālās izmeklēšanas pierādījumu iegūšana, fiksēšana (tīkla iekārtas un resursdatori) un pielietojamie rīki. Digitālās kriminālistikas ieteikumi un labā prakse.	9	8	0	0
Digitālās kriminālistikas analīzes procedūras. Digitālās izmeklēšanas pierādījumu izvērtējums (tīkla iekārtas un resursdatori) un pielietojamie rīki.	9	8	0	0
Incidentu analīzes metodoloģijas, pielietojamie rīki un kiberdraudi.	6	6	0	0
Dažādu sistēmu failu sistēmu, žurnālfailu, sistēmas konfigurācijas analīze un pielietojamie rīki.	8	8	0	0
Mākslīgā intelekta pielietojums digitālās izmeklēšanas procesā.	4	3	0	0
Infrastruktūras aizsardzības veidi (datorsistēmu ievainojamība, operētājsistēmu drošība, datortīklu drošība), tehnoloģijas un pielietojamie rīki.	8	8	0	0
Incidentu pārskatu sagatavošana un pielietojamie rīki.	4	4	0	0
Incidentu pierādījumu prezentēšana un notikumu rekonstrukcija.	4	4	0	0
IT pārvaldības rīku ieviešana digitālās izmeklēšanas procesa uzlabošanai. Ar kiberdrošību saistīti sertifikāti.	8	8	0	0
Kopā:	68	65	0	0

Sasniedzamie studiju rezultāti un to vērtēšana

Sasniedzamie studiju rezultāti	Rezultātu vērtēšanas metodes
Spēj izskaidrot ar digitālās izmeklēšanas procesu saistītās darbības, izklāstīt/izskaidrot digitālos pierādījumus vienkāršā un viegli saprotamā veidā.	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 efektīvi pielietot apgūtās tehnoloģijas digitālās izmeklēšanas procesā.	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 digitālās izmeklēšanas procesu un datu iegūšanas procesu.	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.
Spēj ieviest un uzturēt apgūtās tehnoloģijas dažāda veida industriju uzņēmumos.	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 risināt problēmsituācijas, kurās nepieciešams izmantot dažāda veida digitālās izmeklēšanas pieejas.	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 izstrādāt un paziņot detalizētus un pamatotus izmeklēšanas ziņojumus.	Grupu darbs. // 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		*				