RĪGAS TEHNISKĀ UNIVERSITĀTE

Reģ.Nr.90000068977, Kaļķu iela 1, Rīga, LV-1658, Latvija

Tālr.:67089999; Fakss:67089710, e-pasts:rtu@rtu.lv, www.rtu.lvwww.rtu.lv

Studiju programma "Kiberdrošības inženierija"

Pamatdati

Studiju programmas nosaukums	Kiberdrošības inženierija
Identifikācijas kods	DMK0
Izglītības klasifikācijas kods	45526
Studiju programmas veids un līmenis	Akadēmiskās maģistra studijas
Augstākās izglītības studiju virziens	Informācijas tehnoloģijas, datortehnika, elektronika, telekomunikācijas, datorvadība un datorzinātne
Studiju virziena direktors	Agris Ņikitenko - Doktors, Profesors
Studiju virziena direktora vietnieks	Jurģis Poriņš - Doktors, Profesors
Atbildīgā struktūrvienība	Datorzinātnes un informācijas tehnoloģijas fakultāte
Programmas direktors	Andrejs Romānovs - Doktors, Asociētais profesors
Profesijas klasifikācijas kods	
Īstenošanas forma	Pilna laika
Īstenošanas valoda	Angļu
Apraksts	7. līmenis
Akreditācija	31.05.2013 - 30.06.2023; Akreditācijas lapa Nr. 2020/80
Apjoms kredītpunktos	80.0
Studiju ilgums gados	Pilna laika studijām - 2,0
Iegūstamais grāds un kvalifikācija	inženierzinātņu maģistra grāds kiberdrošībā
Iegūtās kvalifikācijas līmenis	Eiropas kvalifikāciju ietvarstruktūras (EKI) un Latvijas kvalifikāciju ietvarstruktūras (LKI) 7. līmenis
Nepieciešamā iepriekšējā izglītība	bakalaura grāds inženierzinātnēs vai datorzinātnēs, vai profesionālais bakalaura grāds nosauktajām nozaru grupām atbilstošās praktiskās darbības jomās, vai tam pielīdzināma izglītība

Apraksts

Anotācija	Akadēmiskās maģistra studiju programmas “Kiberdrošības inženierija” misija ir nodrošināt teorētisko zināšanu un praktisko iemaņu apguves kopumu, lai studējošie sasniegtu maģistra grādam atbilstošas kompetences kiberdrošības inženierijā. Akadēmiskās maģistra studijās studējošais iegūst nepieciešamās zināšanas, prasmi un kompetenci vispusīgai un efektīvai rīcībai kiberdrošības inženierijas jomā izvēlētajā tautsaimniecības nozarē – IT drošības pārvaldības sistēmu veidošanā, īstenošanā, pilnveidošanā un vadīšanā, izpratni par profesionālo ētiku un sociāli atbildīgu saimniekošanu, plašāku redzesloku, kas veido pamatu turpmākām studijām augstāka līmeņa zināšanu un prasmju iegūšanai. Kiberdrošības speciālista uzdevums organizācijās un uzņēmumos ir pārvaldīt drošības risinājumus, konsultēt lietotājus un nodrošināt ekspertīzi IT drošības jautājumos. Šo uzdevumu īstenošana prasa plaša spektra zināšanas, t.sk. datortīklu, programmatūras, integrētu sistēmu, kritisko infrastruktūru drošību un drošības pārvaldību. Studiju programmas īstenošanā piedalās RTU Datorzinātnes un informācijas tehnoloģijas fakultātes, Enerģētikas un elektrotehnikas fakultātes un Elektronikas un telekomunikāciju fakultātes struktūrvienības. Tehnoloģisko un akadēmisko atbalstu sniedz uzņēmumi Palo Alto Networks un Check Point Software Technologies, nodrošinot iespēju izmantot viņu virtuālās infrastruktūras, kiberpoligonus, datortīklus, kā arī mācību materiālus, vieslekcijas un pasniedzēju un studentu sertifikācijas apmācību par aktuālām kiberdrošības tehnoloģijām un pieejām.
Mērķis	Studiju programmas mērķis ir sagatavot augstākā līmeņa speciālistus kiberdrošībā, kas: 1) izprastu un veidotu uzņēmumu un dažāda veida organizāciju, kā arī sabiedriskās telpas kiberdrošības politiku; 2) veidotu, īstenotu, pārraudzītu un proaktīvi pilnveidotu kiberdrošību nodrošināšanas pasākumus; 3) veiktu starptautiska līmeņa pētījumus kiberdrošībā; un 4) turpinātu izglītību profesionālās kompetences paaugstināšanai vai doktora studiju programmās.
Uzdevumi	Studiju programmas vispārīgie uzdevumi: - nodrošināt starptautiskiem standartiem atbilstošu konkurētspējīgu akadēmisko augstāko izglītību, sagatavot studējošos praktiskam darbam, attīstīt zinātniski pētnieciskā darba iemaņas un veicināt to izmantošanu; - nodrošināt studiju programmas satura, studiju procesa, zinātniski pētnieciskā darba attīstību un izmaiņas atbilstoši tendencēm kiberdrošības jomā, starptautiskajā praksē, zinātnē un didaktikas praksē; - sniegt studentiem vispusīgas zināšanas kiberdrošības inženierijā, veidot speciālista prasmes un attīstīt kompetences atbilstoši darba tirgus prasībām; - veicināt interesi par turpmāko izglītošanos un pilnveidošanos, akadēmisko un profesionālo zināšanu papildināšanu; - rosināt studējošo interesi par sabiedrībā notiekošiem procesiem, stimulēt studentu attīstību par pozitīvu, mūsdienīgu, atbildīgu un rīcībspējīgu personību, kas prot patstāvīgi rīkoties un patstāvīgi pieņemt lēmumus; - veicināt akadēmiskā personāla un studentu savstarpējo mijiedarbību zinātniski pētnieciskā darba veikšanā un iegūto rezultātu praktiskā izmantošanā atbilstoši starptautiskajiem standartiem un tendencēm kiberdrošības jomā; - veicināt un attīstīt akadēmiskā personāla un studentu starptautisko apmaiņu un dalību pētnieciskos projektos.

Studiju rezultāti	Studiju programmas apguves rezultātā absolvents spēj: - identificēt, pamatot un formulēt informācijas tehnoloģiju (IT) drošības nodrošināšanas problēmas; - plānot, ieviest un darbināt kiberdrošības pārvaldības sistēmas; - analizēt, novērtēt un izstrādāt pārvaldības sistēmas, saskaņā ar IT drošības prasībām; - izveidot uzņēmuma digitālo stratēģiju un saskaņot to ar informācijas drošības stratēģiju; - kritiski analizēt sistēmu pārraudzības datus, identificēt un vadīt kiberdrošības riskus; - pielietot IT, kiberdrošības, datizraces un integrācijas rīkus un metodes, kā arī sociālās tehnoloģijas uzņēmuma informācijas aktīvu aizsardzībai; - izstrādāt kiberdrošības apdraudējumu novēršanas organizatoriskos pasākumus un tehniskos risinājumus; - integrēt informācijas drošības risinājumus tīklu, aparatūras, programmatūras datu un procesu līmenī un sintezēt vienotus un sistēmiskus drošības pārvaldības risinājumus; - nodrošināt inženiertehnisko un sociotehnisko sistēmu drošu darbību; - nodrošināt uzņēmuma kritiskās infrastruktūras aizsardzības organizatoriskos pasākumus un tehniskos risinājumus; - novērtēt un nodrošināt informācijas drošības risinājumu atbilstību nozares standartiem un juridiskajām prasībām; - komunicēt, konsultēt, sadarboties un argumentēt kiberdrošības mērķus un rezultātus; - patstāvīgi īstenot zinātniskus pētījumus informācijas tehnoloģijās.
Gala/valsts pārbaudījumu kārtība, vērtēšana	Studiju noslēgumā jāizstrādā Maģistra darbs 20 KP apjomā. Maģistra darbu students izstrādā patstāvīgi studiju pēdējā semestrī, konsultējoties ar darba vadītāju. Nepieciešamības gadījumā studentam tiek organizētas konsultācijas ar speciālistiem atbilstošajā pētījumu nozarē. Maģistra studiju programmas apguvi noslēdz valsts pārbaudījums - maģistra darba aizstāvēšana, kas tiek vērtēts 10 ballu sistēmā. Maģistra darba saturu, tematiku, apjomu, vadītāju, recenzēšanas un aizstāvēšanas kārtību nosaka „Nolikums par maģistra darba izstrādāšanu un aizstāvēšanu". Maģistra darba iespējamo tematu sarakstu apstiprina RTU Informācijas tehnoloģijas institūta padomes sēdē.
Nākamās nodarbinātības apraksts	Studiju programmas absolventi ir gatavi darbam gan valsts un pašvaldību, gan privātajā sektorā - komercsabiedrībās, mazā un vidējā uzņēmējdarbībā. Studiju programma ir piemērota studentiem, kas vēlas kļūt par kiberdrošības analītiķi, kiberdrošības inženieri, kiberdrošības arhitektu, kiberdrošības konsultantu. Absolventi ir sagatavoti tālākai darbībai zinātniskās pētniecības un augstākās izglītības jomā.
Specifiskie uzņemšanas nosacījumi	Pamatprasības: Bakalaura grāds inženierzinātnēs vai datorzinātnēs, vai profesionālais bakalaura grāds nosauktajām nozaru grupām atbilstošās praktiskās darbības jomās, vai tam pielīdzināma izglītība. Papildprasības: sekmīgs vērtējums angļu valodā iepriekšējās izglītības dokumentā, izņemot gadījumus, kad iepriekšējā izglītība iegūta angļu valodā.
Studiju turpināšanas iespējas	Absolvējot maģistra akadēmiskās studijas, izglītošanos var turpināt doktorantūras studiju programmās Latvijas vai ārvalstu augstskolās.

Programmas DMK0 studiju kursi

Nr.	Kods	Nosaukums	Kredītpunkti
A		**Obligātie studiju kursi**	**40.0**
1	DMI745	Ievads kiberdrošībā	4.0
2	DOP715	Informācijas sistēmu drošības pārvaldība	4.0
3	DOP700	Uzņēmumu informācijas tehnoloģijas arhitektūra, lietojumi un integrācija	4.0
4	DMI746	Kiberdrošības risinājumi augstas veiktspējas skaitļošanas vidē	4.0
5	EEI706	Kritisko infrastruktūru vadības pamati	4.0
6	EEI707	Industriālā drošība	4.0
7	DST715	Datortīklu drošība	8.0
8	DPI736	Programmatūras drošība	4.0
9	TRL342	Kriptogrāfijas un datu drošības tehnoloģijas	4.0
B		**Ierobežotās izvēles studiju kursi**	**16.0**
B1		**Profesionālās specializācijas studiju kursi**	**12.0**
1	EEI705	Adaptīvo sistēmu projektēšana	4.0
2	DST717	Inženiertehnisko sistēmu drošība	4.0
3	DMI747	Sociotehnisku sistēmu modelēšana	4.0
4	DMI728	Datizrace un zināšanu atklāšana	4.0
5	DOP711	Projekta vadība	2.0
6	DMI748	Drošās e-komercijas tehnoloģijas	2.0
7	DOP724	Datu integrācijas tehnoloģijas	2.0
B2		**Humanitārie un sociālie studiju kursi**	**4.0**
1	IVZ783	Sociālā atbildība un biznesa ētika	4.0
C		**Brīvās izvēles studiju kursi**	**4.0**
E		**Gala / valsts pārbaudījums**	**20.0**
1	DMI002	Maģistra darbs	20.0