

RTU studiju kurss "Kiberdrošības pamati"

33000 Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte

Vispārējā informācija

Kods	DE0307
Nosaukums	Kiberdrošības pamati
Studiju kursa statuss programmā	Obligātais/Ierobežotās izvēles
Atbildīgais mācītspēks	Andrejs Romānovs - Doktors, Asociētais profesors
Mācītspēks	Jūlija Strebko - Vecākais pasniedzējs Aigars Riekstiņš - Asistents Heinrihs Kristians Skrodelis - Vecākais pasniedzējs
Apjoms daļās un kredītpunktos	1 daļa, 3.0 kredītpunkti
Studiju kursa īstenošanas valodas	LV, EN
Anotācija	Studiju kurss ir paredzēts kiberdrošības zinātnes teorētisko pamatu un praktisko iemaņu apgūšanai, kas nodrošina studentam iespēju efektīvi orientēties mūsdienās Informācijas Tehnoloģijas drošības problēmās. Studiju kurss koncentrējas uz pamatiem un metodēm, kas nodrošina mūsdienīgās kiberdrošības pieejas īstenošanu uzņēmējdarbības vadības kontekstā. Studiju kursā tiek izklāstītas kiberdrošības zinātnes koncepcijas, tehnoloģijas un labākās prakses, IT risku vadības pamatpieejas, informācijas, cilvēkresursu un fizisko IT resursu vadība, kā arī veikta iegūto zināšanu praktiska pielietošana problēmu risināšanai.
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Studiju kursa mērķis ir iepazīstināt studentus ar jaunākajiem sasniegumiem kiberdrošības jomā. Studiju kursa uzdevumi ir sniegt pamatzināšanas un praktiskās iemaņas kiberdrošības pieeju izmantošanā, veicināt studenta spējas un kompetences izvēlēties un pielietot kiberdrošības un IT drošības stratēģijas un vadlīnijas, atbilstošus kiberhigiēnas un IT risku vadības pieejas, definēt to izmantošanu uzņēmējdarbībā, piedāvāt alternatīvus risinājumus.
Patstāvīgais darbs, tā organizācija un uzdevumi	Studentu patstāvīgais darbs ietver analītisko darbu ar mācību literatūru un citiem informācijas avotiem, individuālu un grupas pētījumu un situācijas uzdevumu risināšanu.
Literatūra	Obligātā. / Obligatory: Brian R. Johnson, Patrick J. Ortmeier. Introduction to Security: Operations and Management 5th edition Pearson IT, 2018. 400 pp. Mark S. Merkow, Jim Breithaupt. Information Security: Principles and Practices 2nd Edition Pearson IT, 2014. 368 pp. William Stallings. Effective Cybersecurity: A Guide to Using Best Practices and Standards Addison-Wesley Professional, 2019. 800 pp. Omar Santos. Developing Cybersecurity Programs and Policies 3rd Edition Pearson IT, 2019. 672 pp. Papildu. / Additional: Tony Campbell. Practical Information Security Management: A Complete Guide to Planning and Implementation Apress, 2016. 253 pp. Don Franke. Cyber Security Basics: Protect your organization by applying the fundamentals CreateSpace Independent Publishing Platform, 2016. 101 pp.
Nepieciešamās priekšzināšanas	Pamatzināšanas informācijas tehnoloģijā.

Studiju kursa saturs

Saturs	Pilna un nepilna laika klātienēs studijas		Nepilna laika neklātienēs studijas	
	Kontakt stundas	Patstāv. darbs	Kontakt stundas	Patstāv. darbs
Mūsdienu kiberdrošības tendences un kiberdrošības tehnoloģiskie pamati.	4	4	0	0
Kiberdrošības pārvaldības ietvari, metodoloģijas, standarti un labākās prakses.	8	8	0	0
IT risku un incidentu vadības pamati.	4	4	0	0
Kiberdrošības funkciju (informācijas, cilvēku un fizisko IT resursu) vadības pamati.	16	16	0	0
Piegādes ķēdes un mākoņa drošības vadība.	8	8	0	0
Kopā:	40	40	0	0

Sasniedzamie studiju rezultāti un to vērtēšana

Sasniedzamie studiju rezultāti	Rezultātu vērtēšanas metodes
Spēj definēt, interpretēt un lietot profesionālu terminoloģiju kiberdrošības jomā.	Zinātnisko diskusiju laikā ir parādītas spējas, izmantojot profesionālu terminoloģiju, raksturot problēmu un analizēt risinājumus.
Spēj analizēt un izvēlēties kiberdrošības risinājumus piedāvātā uzdevuma risināšanai.	Kontroldarbu laikā ir parādītas spējas praktiski pielietot iegūtas teorētiskās zināšanas.
Spēj argumentēti diskutēt par kiberdrošības risinājumu izvēli uzņēmuma problēmu risināšanā, tai skaitā prot apkopot kolēģu idejas strādājot grupās, un prezentēt grupas darba rezultātus.	Semināru un praktisko nodarbību darbu laikā, balstoties uz teorētiskajām zināšanām, ir parādītas spējas konstruktīvi diskutēt par risināmo problēmu.

Spēj analizēt konkrētas situācijas un izdarīt patstāvīgus secinājumus par kiberdrošības un IT pārvaldības metodoloģiju izmantošanu uzņēmuma darbībā.	Individuālā pētnieciskā projekta izstādes gaitā ir parādītas spējas piedāvāt alternatīvus risinājumus izvēlētajai problēmai, ka arī veikt šo alternatīvu salīdzinošu analīzi.
Spēj izskaidrot kiberdrošības pieeju pielietojuma būtību, iespējas un nozīmi uzņēmējdarbībā.	Eksāmena laikā ir demonstrēta spēja izanalizēt uzdevuma būtību, kā arī lakoniski un argumentēti piedāvāt atbilstošu kiberdrošības risinājumu uzņēmējdarbības uzdevumiem.

Studiju rezultātu vērtēšanas kritēriji

Kritērijs	% no kopējā vērtējuma
Darbs semināros, diskusijās	15
Kontroldarbi	20
Pētnieciskā projekta izstrāde	25
Eksāmens	40
Kopā:	100

Studiju kursa plānojums

Daļa	KP	Stundas			Pārbaudījumi		
		Lekcijas	Prakt d.	Laborat	Ieskaite	Eksām.	Darbs
1.	3.0	20.0	20.0	0.0		*	