RTU studiju kurss "Kriptogrāfijas un datu drošības tehnoloģijas"

33000 Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte

Vispārējā informācija

Kods	DE0684
Nosaukums	Kriptogrāfijas un datu drošības tehnoloģijas
Studiju kursa statuss programmā	Obligātais/Ierobežotās izvēles
Atbildīgais mācībspēks	Ernests Pētersons - Habilitētais doktors, Profesors
Mācībspēks	Dmitrijs Rjazanovs - Lektors
Apjoms daļās un kredītpunktos	1 daļa, 6.0 kredītpunkti
Studiju kursa īstenošanas valodas	LV, EN
Anotācija	Studiju kursā tiek apgūti ar kriptogrāfijas un datu drošības tehnoloģijām saistītie organizatoriskie un tehnoloģiskie aspekti. Tas sniedz padziļinātas zināšanas, kuras nepieciešamas, lai aizsargātu uzņēmumu informācijas resursus ar kriptogrāfijas tehnoloģiju palīdzību. Tiek izskatīti skaitļu teorijas pamati, elektroniskais paraksts, kriptogrāfija un kriptoanalīze, digitālā tiesu ekspertīze, steganogrāfija, privātums, kriptogrāfijas valūta. Tajā tiek sniegts pārskats par datu aizsardzības uzdevumiem un to risināšanas ceļiem, šifrēšanas algoritmiem uz substitūcijas un permutācijas bāzes, virtuāliem privātiem un bezvadu tīkliem, to drošības protokoliem, autentificēšanu un autorizēšanu.
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Studiju kursa mērķis ir apgūt dažādu kriptogrāfijas un datu drošības tehnoloģiju izmantošanu uzņēmuma informācijas resursu aizsardzībā. Studiju kursa uzdevumi ir attīstīt individuālās un komandas darba iemaņas un prasmes patstāvīgi strādāt ar kriptogrāfijas tehnoloģijām un standartiem un pielietot iegūtās zināšanas praktisko uzdevumu risināšanai.
Patstāvīgais darbs, tā organizācija un uzdevumi	Patstāvīgas literatūras studijas. Studiju procesā tiek apgūts papildmateriāls par dažādu veidu telemātisko sistēmu datu aizsardzības risinājumiem.
Literatūra	Amos R. Omondi.. Cryptography Arithmetic: Algorithms and Hardware Architectures. 2020. Jean-Philippe Aumasson.. Serious Cryptography: A Practical Introduction to Modern Encryption. 2017. Christof Paar, Jan Pelzl.. Understanding Cryptography. A textbook for Students and Practitioners. 2010. Rolf Oppliger.. Contemporary Cryptography. Artech House. 2011. A.Prasad, N. Prasad. . 802.11 WLANs and IP Networking. Security, QoS and Mobility. Artech House. 2008. N. Ferguson, Bruce Schneier.. Practical Cryptography. Wiley Publishing, 2003. Stalling, W.. Data and Computer Communications. Prentice Hall. 2002. RFD 2401. Security Architecture for the Internet Protocol. 1998.
Nepieciešamās priekšzināšanas	Datortīklu pamati.

Studiju kursa saturs

Saturs	Pilna un nepilna laika klātienes studijas		Nepilna laika neklātienes studijas	
	Kontakt stundas	Patstāv. darbs	Kontakt stundas	Patstāv. darbs
Skaitļu teorijas pamati.	8	12	0	0
Datu aizsardzības uzdevumi un to risināšanas veidi.	6	9	0	0
Šifrēšanas algoritmi uz substitūcijas un permutācijas bāzes.	6	9	0	0
Standarts DES un tā stabilitāte.	4	6	0	0
Virtuālie privātie tīkli.	4	6	0	0
Šifrēšanas protokols SSL/TLS.	4	6	0	0
Bezvadu tīkla drošības protokoli.	8	12	0	0
Autentificēšana un autorizēšana. Autentificēšana ar vienreizēju atslēgu.	8	12	0	0
Publiskās atslēgas. Informācijas autentificēšana. Elektroniskais paraksts. Algoritms RSA.	8	12	0	0
Datorvīrusi un antivīrusu programmas.	4	6	0	0
Ugunsmūri un maršrutētāji.	4	6	0	0
Kopā:	64	96	0	0

Sasniedzamie studiju rezultāti un to vērtēšana

Sasniedzamie studiju rezultāti	Rezultātu vērtēšanas metodes
Izprot skaitļu teorijas pamatprincipus un to pielietošanu uzdevumu risināšanā. Spēj raksturot šifrēšanas algoritmus uz substitūcijas un permutācijas bāzes.	Laboratorijas darbs Nr.1. Pārbaudes darbs Nr.1. Eksāmens.
Spēj risināt uzdevumus, izmantojot Eilera funkciju, Eiklīda algoritmu, Fermā teorēmu. Orientējas šifrēšanas algoritmos uz substitūcijas un permutācijas bāzes.	Mājas darbs Nr.1.
Spēj raksturot DES standartu.	Laboratorijas darbs Nr.2. Pārbaudes darbs Nr.2. Eksāmens.

Spēj raksturot "Publiskās atslēgas" (RSA) algoritmu un šifrēšanas protokolu SSL/TLS.	Laboratorijas darbs Nr.3. Pārbaudes darbs Nr.3. Eksāmens.
Izprot tīklu drošības protokolus. Spēj raksturot Informācijas autentificēšanu un Elektroniskā paraksta principus.	Laboratorijas darbs Nr.4. Pārbaudes darbs Nr.4. Eksāmens.
Spēj raksturot PGP algoritmu.	Laboratorijas darbs Nr.5. Pārbaudes darbs Nr.5. Eksāmens.
Spēj raksturot datorvīrusus, antivīrusa programmas un spēj raksturot ugunsmūra izveidošanas metodes.	Laboratorijas darbs Nr.6. Pārbaudes darbs Nr.6. Eksāmens.

Studiju rezultātu vērtēšanas kritēriji

Kritērijs	% no kopējā vērtējuma
Mājas darbi	12
Pārbaudes darbi (kontroldarbi)	28
Laboratorijas darbi	30
Eksāmens	30
Kopā:	100

Studiju kursa plānojums

Daļa	KP	Stundas			Pārbaudījumi		
		Lekcijas	Prakt d.	Laborat	Ieskaite	Eksām.	Darbs
1.	6.0	32.0	0.0	32.0		*	