RTU studiju kurss "Kodēšana un kriptēšana"

33000 Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte

Vispārējā informācija

Kods	DE0840
Nosaukums	Kodēšana un kriptēšana
Studiju kursa statuss programmā	Brīvās izvēles
Atbildīgais mācībspēks	Svitlana Matsenko - Doktors, Docents
Mācībspēks	Jurģis Poriņš - Doktors, Profesors
Apjoms daļās un kredītpunktos	1 daļa, 6.0 kredītpunkti
Studiju kursa īstenošanas valodas	LV, EN
Anotācija	Kļūdu kontroles kodēšana (Error Control Code - ECC) ir viena no rentablām metodēm, kas ir neatņemama jebkuras digitālās komunikācijas sistēmas sastāvdaļa. Mūsdienās gandrīz visas sistēmas izmanto ECC kodus, kas ir integrēti kā sakaru sistēmas shēmas sastāvdaļa, lai panāktu augstu bitu kļūdu īpatsvaru (BER) ar zemām izmaksām. ECC izmanto, lai atklātu kļūdas pārraides laikā sakaru kanālā un šīs kļūdas labot. Šis studiju kurss apvieno kodēšanu, ieskaitot informācijas kodēšanas un pārsūtīšanas, un šifrēšanas izpēti, ieskaitot metodes informācijas aizsardzībai pret nesankcionētu piekļuvi.
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Studiju kursa mērķis ir sniegt teorētiskas un praktiskas zināšanas par instrumentiem, lai saprast, aprakstīt, analizēt un pielietot ECC gan klasiskajā, gan mūsdienu kodēšanas teorijā. Sniegt zināšanas datu šifrēšanā un procesos. Studiju kursa uzdevumi: •Iepazīstināt studējošos ar algoritmiem un matemātiskās kodēšanas metodēm; •Sniegt zināšanas par kodu atlasi un novērtēšanu; •Attīstīt prasmes kriptēšanas un kodēšanas standartu izvēlē; •Sniegt zināšanas par kodu un kriptēšanas programmu izmantošanu; •Iepazīstināt ar kodēšanas sistēmu simulācijām.
Patstāvīgais darbs, tā organizācija un uzdevumi	Studiju kursa ietvaros studentu patstāvīgais darbs tiks organizēts šādi: • risināt akadēmiskā personāla noteiktos uzdevumus, parādot lekcijās iegūto zināšanu izmantošanu, • apkopot un analizēt jaunākos publicētos pētījumu rezultātus par kodēšanu un kriptēšanu, • iegūto teorētisko zināšanu pielietošana matemātiskajā modelī, lai piemērotu kodēšanu un kriptēšanu.
Literatūra	Obligātā literatūra / Obligatory literature: •W. E. Ryan, S. Lin. Channel Codes: Classical and Modern, Cambridge, 2009. •Shu Lin, Daniel J. Costello. Error Control Coding, r., second edition, Prentice-Hall, 2004. •B. Schneier. Applied Cryptography, John Wiley & Sons, 1994. •D. Stinson. Cryptography: Theory and Practice, CRC Press, 1995. Papildliteratūra / Additional literature: •F. J. MacWilliams, N. J. A. Sloane. The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977. •T. K. Moon. Error Correction Coding, 1st Edition, Wiley-Interscience, 2006. •R. E. Blahut. Algebraic Codes for Data Transmission, 1st Edition, Cambridge University Press 2003. •C. W. Huffman, V. Pless. Fundamentals of Error-Correcting Codes, 1st Edition, Cambridge University Press, 2003. •R. Johannesson, Kamil Sh. Zigangirov. Fundamentals of Convolutional Coding., IEEE Press, 1999.
Nepieciešamās priekšzināšanas	Diskrētā matemātika. Varbūtību teorija. Programmēšana. Loģisko iekārtu simulēšanas programmas.

Studiju kursa saturs

Saturs	Pilna un nepilna laika klātienes studijas		Nepilna laika neklātienes studijas	
	Kontakt stundas	Patstāv. darbs	Kontakt stundas	Patstāv. darbs
Ievads informācijā un kodēšanas teorijā.	4	16	0	0
Informācijas teorijas matemātiskās metodes.	6	16	0	0
Lineārie bloku kodi.	10	16	0	0
Konvolūcijas kodi.	16	16	0	0
Zema blīvuma pārības pārbaudes (LDPC) kodi, Turbo kodi.	16	16	0	0
Kriptogrāfija un kriptoanalīze. Šifrēšanas teorijas metodes.	12	16	0	0
Kopā:	64	96	0	0

Sasniedzamie studiju rezultāti un to vērtēšana

Sasniedzamie studiju rezultāti	Rezultātu vērtēšanas metodes
Orientējas dažāda veida kodos.	Tests, eksāmens, praktiskie darbi.

Orientējas kodu matemātiskajos aprakstos un apstrādē.	Tests, eksāmens, praktiskie darbi.
Izprot algoritmus un kodu matemātiskās izstrādes principus.	Tests, eksāmens, praktiskie darbi.
Prot pielietot kodēšanu simulācijas programmās.	Tests, eksāmens, praktiskie un laboratorijas darbi.
Spēj izvēlēties un novērtēt kodus.	Tests, eksāmens, praktiskie darbi.
Izprot kriptogrāfijas un kriptoanalīzes darbības principus.	Tests, eksāmens, praktiskie darbi.

Studiju rezultātu vērtēšanas kritēriji

Kritērijs	% no kopējā vērtējuma
Testi	40
Laboratorijas darbi un praktiskie darbi	30
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.	6.0	40.0	16.0	8.0		*				