RTU Course "Encoding and Encryption"

13104 Telekomunikāciju tīklu katedra

General data

Code	RAE541
Course title	Encoding and Encryption
Course status in the programme	Courses of Free Choice
Course level	Post-graduate Studies
Course type	Academic
Field of study	Electronics and Telecommunications
Responsible instructor	Tālis Celmiņš
Volume of the course: parts and credits points	1 part, 4.0 Credit Points, 6.0 ECTS credits
Language of instruction	LV, RU, DE
Possibility of distance learning	Not planned
Abstract	Characteristics of codes. Simple codes for error detection and error correction. Prefix and suffix codes. Cyclic codes, swapped codes. Applications. Filtering of digital signals. Synchronizaton in TV and message transmission. Methods of encryption.
Goals and objectives of the course in terms of competences and skills	To acquire the following knowledge: •algorithms and mathematical coding methods •selection and evaluation of codes •simulation of coding systems •cryptography selection To develop the following skills: •to select coding and encryption standards •to use coding and encryption software
Structure and tasks of independent studies	Independent work has been intended for: • studying lecture notes • carrying out tasks to develop certain skills
Recommended literature	KK ORTUSā esošie materiāli 1.Теория и практика кодов, контролирующие ошибки. Р. Блейхут."Мир." 1986. 2. Коды исправляющие ошибки.У. Питерсон, Э. Узлдон."Мир." М.1976. 3. Зффективное кодирование. А. А. Новик."Знергия." М. и Л. 1965. 4.Ziņojumu aizsardzība T. Celmiņš. Latvija un perspektīvās telekomunikāciju tehnoloģijas: zinātniski- praktisko rakstu krājums. Rīga, RTU, Telekomunikāciju institūts, 1995. 5Aizsardzības nodrošināšana ziņojumu pārraidē. T. CelmiņšLatvija un perspektīvās telekomunikāciju tehnoloģijas: zinātniski- praktisko rakstu krājums. –Rīga, RTU, Telekomunikāciju institūts, 1996. 6.TRELLIS kodēšana. T. CelmiņšLatvija un perspektīvās telekomunikāciju tehnoloģijas: zinātniski praktisko rakstu krājums. –Rīga, RTU, Telekomunikāciju institūts, 1998. 7.Cannel Coding for Telecommunications.M. BossertWiley. 1999. WEB izmantojamie materiāli 8.http://www.cs.caltech.edu/~umans/522/default.htm 9.http://www-math.cudenver.edu/~wcherowi/courses/m5410/ctcln.html 10.http://theory.csail.mit.edu/~madhu/ST06/scribe/L23_chungc_main.pdf 11.http://math.usask.ca/fvk/CodingTheory.html 12.http://www-math.cudenver.edu/~wcherowi/courses/m4410/codln.html Programmatūras un apraksti 13.http://www.ni.com/academic/circuits.htm
Course prerequisites	Programmable logic controller. Multilevel PLC circuits. Simulation software for logical devices.

Course outline

Theme	Hours
Simple codes.	4
Irregular static codes. Prefix and suffix codes.	6
Block codes. Hamming, Reed–Muller and parity codes.	10
Cyclic codes. Hamming, Golay, Bose –Chaudhuri- Hocquenghem and Reed-Solomon codes.	16
Convolutional codes. Turbo codes.	16
Classified messages. Cryptography and cryptanalysis. Generation and protection of an e-signature.	12

Learning outcomes and assessment

Learning outcomes	Assessment methods
Mastering of knowledge in various types of codes.	Test work.
Mastering of knowledge in code mathematical descriptions and processing.	Test work.
Mastering of knowledge in algorithms and mathematical code development.	Test work.
Mastering of knowledge in simulation of coding units.	Test work. Labs.
Mastering of knowledge in code selection and evaluation.	Test work.

Mastering of knowledge in cryptography.	Test work.

Study subject structure

Part	CP	ECTS	Hours per Week			Tests			Tests (free choice)		
			Lectures	Practical	Lab.	Test	Exam	Work	Test	Exam	Work
1.	4.0	6.0	2.5	1.0	0.5		*				