RTU Course "Encoding and Encryption"

13104 null

General data

Code	RAE541
Course title	Encoding and Encryption
Course status in the programme	Courses of Free Choice
Responsible instructor	Svitlana Matsenko
Academic staff	Jurģis Poriņš
Volume of the course: parts and credits points	1 part, 4.0 Credit Points, 6.0 ECTS credits
Language of instruction	LV, EN
Annotation	Error control coding (ECC) is one of the cost-effective methods, which is are a vital indispensable part of any digital communication system. Nowadays almost all systems use EEC codes being integrated as a part of the communication system scheme to achieve a high bit error rate (BER) with a low cost. ECC is used to detect errors during transmission over the communication channel and, possibly, to correct these errors. This study course combines encoding including the study of information coding and transfer and encryption including the techniques for protecting information from unauthorized access.
Goals and objectives of the course in terms of competences and skills	The aim of the study course is to provide theoretical and practical knowledge of tools to understand, describe, analyze and apply ECC in both classical and modern coding theory. Provide knowledge of data encryption and processes. Tasks of the study course: • To acquaint students with algorithms and mathematical coding methods; • To provide knowledge about code selection and evaluation; • To develop skills in choosing encryption and encryption standards; • To provide knowledge about the use of code and encryption programs; • To introduce coding system simulations.
Structure and tasks of independent studies	Within the study course, students' independent work will be organized as follows: • to solve the tasks defined by the academic personnel, showing the use of the knowledge acquired in the lectures, • summarize and analyze the latest published research results on encoding and encryption, • applying the acquired theoretical knowledge to a mathematical model to apply encoding and encryption.
Recommended literature	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.
Course prerequisites	Discrete Mathematics. Probability theory. Programming. Simulation software for logical devices.

Course contents

Content	Full- and part-time intramural studies		Part time extramural studies	
	Contact Hours	Indep. work	Contact Hours	Indep. work
An introduction to information and coding theory.	4	16	0	0
Mathematical methods of information theory.	6	16	0	0
Linear block codes.	10	16	0	0
Convolutional codes.	16	16	0	0
Low-density parity-check (LDPC) codes, Turbo codes.	16	16	0	0
Cryptography and cryptanalysis. Methods of the theory of encryption.	12	16	0	0
Total:	64	96	0	0

Learning outcomes and assessment

Learning outcomes	Assessment methods
Students are able to orient in different types of codes.	Test. Practical work. Exam.
Students are able to orient in code mathematical descriptions and processing.	Test. Practical work. Exam.

Students are able to model coding algorithms.	Test. Practical work. Exam.
Students can work with simulations of coding units.	Test. Practical and laboratory work. Exam.
Students are able to select and evaluate codes.	Test. Practical work. Exam.
Students are able to explain the principles of cryptography and cryptanalysis.	Test. Practical work. Exam.

Evaluation criteria of study results

Criterion	%
Tests	40
Laboratory work and practical tasks	30
Exam	30
Total:	100

Study subject structure

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