|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **UČNI NAČRT PREDMETA / COURSE SYLLABUS** | | | | | | | | | | | | | | | | | |
| **Predmet:** | | | Informacija in kodi | | | | | | | | | | | | | | |
| **Course title:** | | | Information Theory and Coding | | | | | | | | | | | | | | |
|  | | | | |  | | | | | | | |  | |  | | |
| **Študijski program in stopnja**  **Study programme and level** | | | | | **Študijska smer**  **Study field** | | | | | | | | **Letnik**  **Academic year** | | **Semester**  **Semester** | | |
| Podiplomski magistrski študijski program druge stopnje Elektrotehnika | | | | | Avtomatika in informatika | | | | | | | | 1 | | 2 | | |
| 2nd cycle masters study programme in Electrical Engineering | | | | | Control systems and computer engineering | | | | | | | | 1 | | 2 | | |
|  | | | | | | | | | | | | | | | | | |
| **Vrsta predmeta / Course type** | | | | | | | | | | | | Obvezni-strokovni / Compulsory professional | | | | | |
|  | | | | | | | | | | | |  | | | | | |
| **Univerzitetna koda predmeta / University course code:** | | | | | | | | | | | | 64207 | | | | | |
|  | | | | | | | | | | | | | | | | | |
| **Predavanja**  **Lectures** | **Seminar**  **Seminar** | | | **Vaje**  **Tutorial** | | | **Klinične vaje**  **work** | | | | **Druge oblike študija** | | | **Samost. delo**  **Individ. work** | |  | **ECTS** |
| **45** | **0** | | | **30** | | |  | | | |  | | | **75** | |  | **6** |
|  | | | | | | | | | | | | | | | | | |
| **Nosilec predmeta / Lecturer:** | | | | | Simon Dobrišek | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | |
| **Jeziki /**  **Languages:** | | **Predavanja / Lectures:** | | | | slovenščina in po potrebi angleščina / Slovene and English, if necessary | | | | | | | | | | | |
| **Vaje / Tutorial:** | | | | slovenščina in po potrebi angleščina / Slovene and English, if necessary | | | | | | | | | | | |
| **Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:** | | | | | | | | |  | **Prerequisites:** | | | | | | | |
| Vpis v letnik. | | | | | | | | |  | Enrolment in the year of the course. | | | | | | | |
|  | | | | | | | |  | |  | | | | | | | |
| * Uvod: definicija informacije, koda, kodiranja in komunikacijskega sistema. * Entropija: diskretni naključni sistemi, entropija diskretne naključnih spremenljivk, entropija zveznih naključnih spremenljivk. * Informacija: povprečna lastna informacija, povprečna medsebojna informacija diskretnih spremenljivk, povprečna medsebojna informacija zveznih spremenljivk. * Diskretni viri informacije: entropija stacionarnega vira, ergodični stacionarni viri, vir brez spomina, vir s spominom, odvečnost vira. * Kodiranje vira informacije: enakomerni in neenakomerni kodi, Kraft-McMillanova neenačba, Huffmanov kod, aritmetični kod , kod LZW. * Tajno kodiranje: kriptografski sistemi s tajnim ključem, kriptografska sistema DES in AES, kriptografski sistemi z javnim ključem, kriptografski sistem RSA, digitalni podpis. * Komunikacijski kanali I: zvezni komunikacijski kanali, kapaciteta zveznega kanala, diskretni komunikacijski kanali, kapaciteta diskretnega kanala brez spomina. * Komunikacijski kanali II: dekodiranje z odkrivanjem napak, dekodiranje s popravljanjem napak, optimalni postopki dekodiranja, Shannonov izrek o varnem kodiranju, obrat Shannonovega izreka. * Varno kodiranje: linearni bločni kodi, ciklični kodi, Hammingov kod, Golayev kod, kodi Reeda in Mullerja, konvolucijski kodi, Viterbijev algoritem, Turbo kod | | | | | | | |  | | * Introduction: definition of information, code, coding and communication system. * Entropy: discrete random systems, entropy of a discrete random variable, entropy of a continuous random variable. * Information: average information, mutual information of two discrete variables, mutual information of two continuous variables. * Discrete information sources: entropy of a stationary source, ergodic stationary sources, memoryless sources, sources with memory, and source redundancy. * Information source coding: fixed-length and variable-length coding, Kraft – McMillan inequality, Huffman code, arithmetic code, LZW code. * Secrecy coding: cryptosystems with a secret key, DES and AES cryptosystems, cryptosystems with a public key, RSA cryptosystem, digital signature. * Communication channels I: continuous communication channels, the capacity of a continuous communication channel, discrete communication channels, the capacity of a discrete communication channel. * Communication channels II: error-detecting codes, error-correcting codes, optimal decoding, Shannon theorem of secure coding, inversion of Shannon theorem. * Channel coding: linear block codes, cyclic codes, Hamming codes, Golay codes, the Reed-Muller codes, convolutional codes, the Viterbi algorithm, Turbo codes. | | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Temeljni literatura in viri / Readings:** | | | | | |
| 1. N. Pavešić: Informacija in kodi, (2. izdaja), Založba FE in FRI, 2010. 2. V. Štruc, S. Dobrišek: Informacija in kodi : dopolnilni učbenik z vajami. 1. izd., Založba FE, 2016 3. T. M. Cover, J. A. Thomas: Elements of Information Theory, Wiley-Interscience, New York, 2006. 4. Roberto Togneri, Christopher J. S. deSilva: Fundamentals of information Theory and Coding Design, Chapman & Hall / CRC, 2002. | | | | | |
| **Cilji in kompetence:** | |  | | **Objectives and competences:** | |
| Seznaniti študenta z najpomembnejšimi koncepti in metodami iz teorije informacij, kodiranja vira, kriptografije in kodiranja kanala. | |  | | To provide students with an understanding of the most important concepts and methods from information theory, source coding, cryptography, and channel coding. | |
| **Predvideni študijski rezultati:** | | |  | **Intended learning outcomes:** | |
| Znanje in razumevanje:  Po zaključku tega predmeta bo študent zmožen izkazati znanje in razumevanje:   * gradnje matematičnih modelov za opisovanje poglavitnih pojavov v tehničnih komunikacijskih sistemih, * mere informacije in ostalih parametrov, ki se uporabljajo za kvantitativno opisovanje komunikacijskih in informacijskih sistemov, * kodiranja informacij in kriptografije.   Uporaba znanja:  Pridobljeno znanje bo študent lahko uporabil pri gradnji kodirnikov informacije in elektronskem poslovanju ter uporabi digitalnih potrdil pri preverjanju istovetnosti oseb in šifriranju sporočil. Študent bo zmožen kritično ovrednotiti skladnost med pridobljenim znanjem ter uporabo konceptov iz teorije informacij in metod kodiranja vira, kriptografije na področjih telekomunikacij, avtomatike in kibernetike.  Prenosljive spretnosti:   * uporabe literature ter drugih virov s področja teorije informacij in kodiranja, * uporaba računalniških razvojnih orodij in okolij za programiranje (pisanje programov v enem od programskih jezikov C/C++, C#, Java, Python ali z uporabo razvojnega okolja MatLab), * reševanja problemov: analiza problema, načrtovanje algoritma, implementacija programa in testiranje programa, * dela v skupini: organizacija in vodenje skupine, aktivno sodelovanje v skupini. | | |  | Knowledge and understanding:  After completing this course the student will be able to demonstrate a knowledge and understanding of the:   * construction of the mathematical models used to describe the main phenomena in technical communication systems, * information measure and other parameters used for a quantitative description of communication and information systems, * information coding and cryptography.   The use of knowledge:  The student will be able to use the acquired knowledge to construct information encoders, in e-commerce as well to manage digital certificates for digital-identity management and encrypting messages. The student will be able to critically evaluate the consistency between the acquired knowledge and the application of the concepts of information theory, coding and cryptography in the fields of telecommun­ications, automation, control, and cybernetics.  Transferable skills:   * the use of literature and other resources in the fields of information theory and coding; * the use of development tools and environments for computer programming (writing computer programs in different programming languages, such as C/C++, C#, Java, Python, or using the Matlab development environment); * problem solving: problem analysis, algorithm design, implementation and testing of a program; * group work: the organisation and management of groups, active participation in groups. | |
|  | | |  |  | |
| **Metode poučevanja in učenja:** | | |  | **Learning and teaching methods:** | |
| * predavanja, * laboratorijske vaje in projekti, * reševanje domačih nalog. | | |  | * lectures, * laboratory exercises and projects, * coursework. | |
| **Načini ocenjevanja:** | Delež (v %) /  Weight (in %) | | | | **Assessment:** |
| Način: domače naloge, laboratorijske vaje, projekt, pisni izpit, ustni izpit.  Ocene od 1 do vključno 5 so negativne, ocene od vključno 6 do 10 so pozitivne.  Pozitivna ocena laboratorijskih vaj je pogoj za pristop k izpitu.  Prispevki k oceni:   * domače naloge, * laboratorijske vaje in projekt, * pisni izpit, * ustni izpit. | 10%  30%  30%  30% | | | | Type: homework, laboratory exercises, project, written exam, oral exam.  Negative grades: from 1 to 5, positive grades: from 6 to 10.  Positive evaluation of laboratory exercises is a prerequisite for the exam.  Contributions to the final grade:   * coursework, * laboratory exercises and project, * written exam, * oral examination. |
| **Reference nosilca / Lecturer's references:** | | | | | |
| 1. ŠTRUC, Vitomir, DOBRIŠEK, Simon. Informacija in kodi : dopolnilni učbenik z vajami. 1. izd. Ljubljana: Založba FE, 2016 2. DOBRIŠEK, Simon. Pametni nadzorni sistemi : je to grožnja umetne inteligence. V: 1. dnevi prava zasebnosti in svobode izražanja, [Kranjska Gora, 9. in 10. april 2015]. Zbornik 2015. 1. natis. Ljubljana: IUS Software, GV založba, 2015, str. 134-138. 3. GOLOB, Žiga, ŽGANEC GROS, Jerneja, ŽGANEC, Mario, VESNICER, Boštjan, DOBRIŠEK, Simon. FST-based pronunciation lexicon compression for speech engines. International journal of advanced robotic systems, ISSN 1729-8814, 2012, vol. 9, no. 211, str. 1-9. 4. DOBRIŠEK, Simon (intervjuvanec). Jezikovni pogovori. Ljubljana: Radio Slovenija, Program ARS, 16. 10. 2012. 5. DOBRIŠEK, Simon, ŽIBERT, Janez, PAVEŠIĆ, Nikola, MIHELIČ, France. An edit-distance model for the approximate matching of timed strings. IEEE transactions on pattern analysis and machine intelligence, ISSN 0162-8828. [Print ed.], Apr. 2009, vol. 31, no. 4, str. 736-741. | | | | | |