	UČNI NAČRT PREDMETA/COURSE SYLLABUS
Predmet	**Kibernetika in kibernetska varnost**
Course title	**Cybernetics and Cyber Security**

Študijski program in stopnja **Study programme and level**	**Študijska smer** **Study field**	**Letnik** **Academic year**	**Semester** **Semester**
Poslovna ekonomija in upravljanje	Upravljanje in razvoj informacijskih sistemov	2.	3.
Business Economics and Management	Management and Development of Information Systems	2nd	3rd

Vrsta predmeta/Course type izbirni / elective

Univerzitetna koda predmeta/University course code 3_PEU_IP_UN7_URIS

Predavanja **Lectures**	**Seminar** **Seminar**	**Sem. vaje** **Tutorial**	**Lab. vaje** **Laboratory work**	**Teren. vaje** **Field work**	**Samost. delo** **Individ. work**	**ECTS**
15	10				425	15

Nosilec predmeta/Lecturer: izr. prof. dr. Ivan Gerlič, doc. dr. Branko Kaučič

Jeziki/ Languages:	
Predavanja/Lectures:	slovenski/Slovenian
Vaje/Tutorial:	slovenski/Slovenian

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**
• Pogoj za vključitev v delo je vpis v drugi letnik študijskega programa. • Študent mora pred izpitom pripraviti in predstaviti raziskovalno nalogo.	• The prerequisite for participation is enrolment in the second year of study. • Student has to prepare, present and defend a research paper before the examination.

Vsebina:	**Content (Syllabus outline):**
• *Uvod:* Osnove kibernetike. Razvoj kibernetske teorije. Osnove teorije sistemov. • *Bazična kibernetika:* proučevanje sistemov nadzora in odkrivanje osnovnih načel v umetni inteligenci, robotiki, nadzornih sistemih, računalniškem vidu… • *Aplikativna kibernetika:* kibernetika v biologiji, računalništvu, inženirstvu, upravljanju, matematiki…	• *Introduction:* Fundamentals of Cybernetics. Development of cybernetic theory. Fundamentals of systems theory. • *Basic cybernetics:* study of control systems and discovery of basic principles in artificial intelligence, robotics, control systems, computer vision… • *Applied cybernetics:* cybernetics in biology, computer science,

• *Kompleksni sistemi:* teorija kompleksnosti. • *Kibernetska varnost:* opredelitev kibernetske varnosti, kibernetski napadi, tveganja kibernetskega prostora. • *Zagotavljanje kibernetske varnosti:* organizacije odgovorne za kibernetsko varnost, strategije in sodobni aspekti kibernetske varnosti, informiranost o kibernetski varnosti in kriminaliteti. • *Strategija kibernetske varnosti v SLO in EU.*	engineering, management, mathematics… • *Complex systems:* complexity theory. • *Cyber security:* definition of cyber security, cyber-attacks, risks in cyberspace. • *Ensuring cyber security:* organizations responsible for cyber security, cyber security strategies, cyber security information and cybercrime awareness. • *Cyber security strategy in SLO and the EU.*

Literatura in viri/Readings:

Temeljna literatura/Basic literature

- Diogenes, J., Ozkaya, E. (2019). *Cybersecurity – Attack and Defense Strategies*. Packt.
- Cardon, A. (2018). *Beyond Artifical Inteligence*. IST, Wiley.
- Bernik, I., Pritan, K. (2012). *Kibernetska kriminaliteta, informacijsko bojevanje i kibernetski terorizem.* Ljubljana: Fakulteta za varnosten vede Univerze v Mariboru.
- Završnik, A. (2015). *Kibernetska kriminaliteta*. Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti UNI Ljubljana.

Priporočljiva literatura/Recommended literature

- Ozkaya, E. (2019). *Cybersecurity: The Beginers Guide*. Packt.
- Gerlič, I. (2020). *Računalništvo in informatika v zdravstvu*. Univerza v Novem mestu.
- Ivanuša, T. (2013). *Kibernetska varnost sistemov*. Ljubljana: Zavod za varnostne strategije Univerze v Mariboru.
- Si-CERT. (2019). *Poročilo o omrežni varnosti za leto 2019*. Ljubljana: Si-CERT.
- Republika Slovenija. (2016). *Strategija kibernetske varnosti*. Digitalna Slovenija.
- Spagnolo, G. and all. (2020). *Kibernetska varnost*. Digitalno inovacijsko stičišče Slovenije.
- Republika Slovenija. (2018). Zakon o informacijski varnosti (ZInfV). Uradni list 011-02/18-4/13.
- Tomše, S., Markelj B. (2020). Informacijska varnost: Etično hekanje. GV založba
- Dreven, M. And all (2020). Informacijska varnost: Izzivi sodobne tehnologije. GV založba.

Cilji in kompetence:	Objectives and competences:
Učna enota prispeva predvsem k razvoju naslednjih splošnih in specifičnih kompetenc: • poglobljeno poznavanje teorij in aplikativne razvojno raziskovalne prakse kibernetike in kibernetske varnosti, • usposobljenost za kreativno in samostojno znanstveno raziskovalno in razvojno delo, reševanje zahtevnih in	*The learning unit mainly contributes to the development of the following general and specific competences:* • in-depth knowledge of the theories and applied research and development practices of cybernetics and cyber security, • the ability to engage in creative and independent scientific research and development, to solve demanding and

kompleksnih problemov in vodenje raziskovalnih in razvojnih projektov, • usposobljenost za samostojno in timsko raziskovalno in razvojno delo v razvojnih in interdisciplinarnih skupinah, za uporabo znanstvenih pristopov pri delu in za obvladanje sodobnih razvojnih postopkov na področju računalništva in informatike s poudarkom na kibernetski varnosti, • uporaba modernih orodij in tehnik pri reševanju in predstavitvi problemov kibernetske varnosti, • usposobljenost za sintezo in interpretacijo v raziskavah pridobljenih podatkov ter prenos znanja v konkretno delovno in znanstveno-raziskovalno okolje.	complex problems and to manage research and development projects, • the ability to carry out independent and team-oriented research and development work in development and interdisciplinary groups, to apply scientific working methods and to master modern development procedures in the fields of computer science and informatics with a focus on cyber security, • the use of modern tools and techniques in solving and presenting cyber security problems, • the ability to synthesize and interpret data obtained in research and to apply knowledge to a specific work and scientific research environment.

Predvideni študijski rezultati:	Intended learning outcomes:
Študent/študentka: • pozna kibernetske teorije in paradigme kibernetske varnosti, • se usposobi za kritično presojo in analizo kibernetskih sistemov in kibernetske varnosti, • razume pomen kibernetike v povezavi s kibernetsko varnostjo, • razvija sposobnosti načrtovanja in izvedbe raziskovalnega dela, analize in interpretacije podatkov pomembnih za kibernetsko varnost, preprečevanje kibernetskih napadov in tveganj kibernetskega prostora, • razvije sposobnost za reševanje poslovnih problemov v povezavi z kibernetsko varnostjo.	*Students:* • are familiar with the importance of cyber theories and paradigms of cyber security, • develop skills for critical assessment and analysis of cyber systems and cyber security, • recognise the importance of cybernetics in relation to cyber security, • develop skills in planning and conducting research, analysing and interpreting data relevant to cyber security, prevention of cyber attacks and cyber risks, • develop skills in solving business problems related to cyber security.

Metode poučevanja in učenja:	Learning and teaching methods:
• predavanja z aktivno udeležbo študentov (razlaga, diskusija, vprašanja, primeri, reševanje problemov), • projektni seminar, • individualne in skupinske konsultacije (diskusija, dodatna razlaga, obravnava specifičnih vprašanj), • oblikovanje portfolija in samostojen študij (motiviranje, usmerjanje,	• lectures with active student participation (explanation, discussion, questions, examples, problem solving), • project work seminar, • individual and group consultations (discussion, further explanation, addressing specific issues), • designing a portfolio and independent study (motivating, directing, self-

samoopazovanje, samouravnavanje, refleksija, samoocenjevanje).	observation, self-regulation, reflection, self-assessment).

Načini ocenjevanja:	Delež (v %) Weight (in %)	Assessment:
Načini: • temeljna ali aplikativna raziskovalna naloga z zagovorom (obseg 30.000 znakov). Ocenjevalna lestvica: uspešno, neuspešno.	100 %	Types: • fundamental or applied research paper with defence (30,000 characters). Grading scheme: successful, unsuccessful.