UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Uvod v kibernetsko varnost
Course title:	Introduction to Cybersecurity

Študijski program in stopnja **Study programme and level**	**Študijska smer** **Study field**	**Letnik** **Academic year**	**Semester** **Semester**
Informatika v sodobni družbi, visokošolski strokovni študijski program prve stopnje in Računalništvo in spletne tehnologije, visokošolski študijski program prve stopnje	-	Drugi ali tretji	Četrti ali šesti
Informatics in Contemporary Society, first cycle Professional Study Programme and Computer science and web technologies, first cycle Professional Study Programme	-	Second or third	Fourth or sixth

Vrsta predmeta / Course type	Izbirni/ Elective
Univerzitetna koda predmeta / University course code:	1-ISD-RST-VS-UKV-2022-12-16

Predavanja **Lectures**	**Seminar** **Seminar**	**Vaje** **Tutorial**	**Klinične vaje** **work**	**Druge oblike študija**	**Samost. delo** **Individ. work**	**ECTS**
30	-	30	-	-	120	6

Nosilec predmeta / Lecturer:	

Jeziki / Languages:	**Predavanja / Lectures:**	slovenski, angleški / Slovene, English
	Vaje / Tutorials:	slovenski, angleški / Slovene, English

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisits:**
Študent/študentka mora pred pristopom k izpitu imeti pozitivno ocenjene vaje.	Positively evaluated exercises are prerequisites for the exam.

Vsebina:

- Temelji kibernetske varnosti
- Obrambni in varnostni sistemi
- Grožnje in ranljivosti
- Razumevanje tveganj
- Odziv na incidente
- Upravljanje kibernetske varnosti in skladnost
- Kibernetska kriminaliteta
- Kibernetsko bojevanje in terorizem

Content (Syllabus outline):

- Cybersecurity Foundations
- Defending and Securing Systems
- Threats, Vulnerabilities
- Risk Management
- Incident Response
- Cybersecurity Governance and Compliance
- Cybercrime
- Cyberwarfare and cyberterrorism

Temeljni literatura in viri / Readings:

- PRISLAN, Kaja, BERNIK, Igor. *Informacijska varnost in organizacije*. 1. izd. Maribor: Univerzitetna založba Univerze; Ljubljana: Fakulteta za varnostne vede, 2019
- BERNIK, Igor, PRISLAN, Kaja. Study of organized cybercrime and information warfare. V: LEVNAJIĆ, Zoran (ur.). *Facing ICT challenges in the era of social media*. Frankfurt am Main: PL Academic Research, 2014, str. 67-82
- Matej Kovačič. *Crash course on cybersecurity: a manual for surviving in a networked world.* University of Nova Gorica Press. ISBN: 978-961-7025-24-8 (PDF), 2022.
- Prosto dostopna poročila organizacij kot so CERT.si, Safe.si, UN, Sans Newsbytes, Sophos, ipd.
- ISO/IEC 27001:2022: *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.*

Dodatna literature:

- ISO/IEC 27002:2022: *Information security, cybersecurity and privacy protection — Information security controls.*

Cilji in kompetence:

Cilji učne enote so:

- Osvojiti razumevanje kibernetske varnosti kot osnovnega aspekta celovitega varovanja informacij za doseganje delovnih ciljev in globalno povezljivost.
- Seznaniti slušatelje s potrebami in vzroki za varovanje informacijskega premoženja.
- Razumeti procese varnega izmenjevanja informacij in potrebnih tehnologije.
- Uporabiti spoznanja v doseganju osebnih in organizacijskih ciljev ter razumeti osnovo za varno delu v realnem in kibernetskem prostoru z zmanjševanjem možnosti zlorabe informacij in zasebnosti.

Objectives and competencies:

The objectives of the study units are:

- To understand cyber security as a basic aspect of comprehensive information security for achieving work goals and global connectivity.
- To introduce the needs and reasons for protecting information assets.
- Understand the processes of secure information exchange and the technologies which can be used.
- Use knowledge to achieve personal and organizational goals, and understand the basis for safe work in real and cyberspace by reducing the possibility of misuse of information and privacy.

Učna enota prispeva k razvoju naslednjih splošnih kompetenc: ▪ Usposobljenost za samostojno in avtonomno uporabo, nadzor in vzdrževanje informacijsko komunikacijske tehnologije v organizaciji; ▪ Poznavanje in razumevanje širokega nabora aplikacij informacijsko komunikacijske tehnologije v sodobni družbi ter razumevanje interakcij med informacijsko komunikacijsko tehnologijo in sodobno družbo; ▪ Sposobnost uporabe znanja v praksi; *In predmetno-specifičnih kompetenc:* ▪ Razumevanje varovanja informacij, ohranjanja njihove vrednosti in načinov zlorab informacij v realnem in kibernetskem prostoru. ▪ Seznanjenost z IT tehnologijami in načinom uporabe le-te v informacijski družbi in potrebe ter vzroke za varovanje informacijskega premoženja. ▪ Razumevanje aktualnih domačih in mednarodnih raziskav za pripravo na odzivanje pred kibernetskimi grožnjami.	The instructional unit contributes to the development of the following general competencies: ▪ The ability to independently and autonomously use, control and maintain ICT within the organization. ▪ Knowledge and understanding of a wide range of applications of ICT in modern society and an understanding of the interaction between information and communication technology and modern society. ▪ The ability to apply knowledge in practice. *And subject-specific competencies:* ▪ Understanding cybersecurity, preserving their values and ways of misusing the information in the physical world and cyberspace. ▪ Familiarize yourself with IT technology, how to use it in the information society, and the needs and reasons for protecting information assets. ▪ Understanding of current domestic and international research to prepare for responding to cyber threats.
Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: *Sposobnost študenta/študentke bo:* • razumeti proces zagotavljanja varnosti v kibernetskem prostoru • uporabljati sodobne varnostne tehnologije za varno delo v kibernetskem prostoru • analizirati stanje in oceniti varnostna tveganja • razumeti kibernetsko kriminaliteto, kibernetsko bojevanje in kibernetski terorizem	Knowledge and understanding: The students will be able to: • understand the process of ensuring security in cyberspace • use of modern safety technologies for safe work in the cyberspace • analyze the situation and assess security risks • • understand cybercrime, cyberwarfare and cyberterrorism
Metode poučevanja in učenja:	**Learning and teaching methods:**

• *predavanja* z aktivno udeležbo študentov (razlaga, diskusija, vprašanja, primeri, reševanje problemov) • *laboratorijske vaje*	• lectures with the active participation of students (explanation, discussion, questions, examples, problem solving) • laboratory work

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt): • pisni izpit • poročila laboratorijskih vaj	 60 % 40 %	Type (examination, oral, coursework, project): • written exam • report on laboratory exercises