UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Kibernetska varnost
Course title:	Cyber Security

Študijski program in stopnja Study programme and level	Študijska smer Study field	Letnik Academic year	Semester Semester
Kibernetska varnost, magistrski študijski program druge stopnje	-	Prvi	Drugi
Cyber Security, second cycle Masters Study Programme	-	First	Second

Vrsta predmeta / Course type	Obvezni / Obligatory
Univerzitetna koda predmeta / University course code:	5-KV-MAG-KV-2021-12-14

Predavanja Lectures	Seminar Seminar	Vaje Tutorial	Klinične vaje work	Druge oblike študija	Samost. delo Individ. work	ECTS
30	-	45	-	-	105	6

Nosilec predmeta / Lecturer:	prof. dr. Igor Bernik
Jeziki / Languages: Predavanja / Lectures:	slovenski, angleški / Slovene, English
Vaje / Tutorial:	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 in seminarsko nalogo.	Positively evaluated exercises and seminar paper are a prerequisite for exam.

Vsebina:	Content (Syllabus outline):
• Sodobna kibernetska varnost • Nacionalna in mednarodne strategije kibernetske varnosti • Skladnost in varstvo osebnih podatkov • Sodobna tehnologija v kibernetskem prostoru, uporaba in nevarnosti za uporabnike; poslovni vidiki • Mednarodno okolje in kibernetska varnost • Nadzor v mednarodnih podatkovnih povezavah	• Modern cybersecurity • National and international cyber security strategies • Compliance and personal data protection • Modern technology in cyberspace, use and risks to users; the business aspects • International Environment and cybersecurity • Control of international data links

- Zrelostni model kibernetske varnosti skupnosti
- Zakonodajni okviri in mednarodna usklajenost kibernetske varnosti
- Zavarovanje kibernetske infrastrukture
- Soodvisnost kritične infrastrukture, modeli in študije primerov soodvisnosti
- Kibernetska kriminaliteta
- Spoznanja o kibernetski kriminaliteti
- Organizirana kriminaliteta v kibernetskem prostoru
- Kibernetsko bojevanje
  - meddržavno in vojaško področje
  - poslovna sfera
  - civilna sfera
- Dogajanja na področju kibernetskega bojevanja
- Kibernetski terorizem in varnostne implikacije kibernetskega terorizma

- Community Cyber Security Maturity Model
- Cybersecurity legislative frameworks and international consistency
- Insurance of cyber infrastructure
- Critical infrastructures and interdependencies, models and case studies for interdependencies
- Understanding cybercrime
- Knowledge about cybercrime
- Organized Crime in cyberspace
- Cyberwarfare
  - interstate and military sphere
  - business sphere
  - civil sphere
- Developments in the field of cyberwarfare
- Cyberterrorism and security implications from the onset of cyberterrorism

Temeljni literatura in viri / Readings:

- Bernik, I. (2014) Cybercrime and cyberwarfare, (Focus series). London: ISTE; Hoboken: Wiley.
- Tomažič, S., Bernik, I. (2019). Cyberattack response model for the nuclear regulator in Slovenia. *Journal of universal computer science*, ISSN 0948-6968, 2019, vol. 25, no. 11, str. 1437-1457.
- Strategije kibernetske varnosti, zakonodaja, poročila različnih organizacij, kot so CERT, UN, Sans Newsbytes in Sophos Naked Security ter podobno.

Cilji in kompetence:

Cilji učne enote so:

- Nadgraditi razumevanje kibernetske varnosti kot osnovnega aspekta celovitega varovanja informacij za doseganje delovnih ciljev in globalno povezljivost.
- Seznaniti slušatelje s tehnologijami in načinom uporabe le te v informacijski družbi in potrebe ter vzroke za varovanje informacijskega premoženja.
- Nadgraditi obvladovanje in razumevanje procesov varnega izmenjevanja informacij, potrebnih tehnologije, zagotavljanja varnega izmenjevanje informacij.

Objectives and competences:

The objectives of the study units are:

- Upgrade understanding of information security as a basic aspect of a comprehensive information security for achieving work goals and global connectivity.
- To introduce the technology and how to use it in the information society and the needs and reasons for protecting information assets.
- Upgrade the understanding and control of safe exchange of information and technologies necessary to provide secure exchange of information.
- Upgrade knowledge in achieving personal and organizational goals, and

- Nadgraditi uporabnost spoznanj v doseganju osebnih in organizacijskih ciljev ter podati osnovo za varno delu v realnem in kibernetskem prostoru z zmanjševanjem možnosti zlorabe informacij in zasebnosti.

Učna enota prispeva k razvoju naslednjih splošnih in predmetno specifičnih kompetenc:
Splošne kompetence:

- Razumevanje pomena kibernetske varnosti.
- Sposobnost identifikacije kibernetskih varnostnih tveganj ter izdelave predlogov za ukrepanje in zaščito na osnovi identificiranih tveganj.
- Sposobnost pridobivanja, selekcije, analize informacij in zmožnost njihove interpretacije za celovito reševanje problemov, izzivov in incidentov s področja kibernetske varnosti.
- Sposobnost iskanja podatkov in virov za potrebe upravljanja kibernetske varnosti.
- Sposobnost poslovnega komuniciranja, skupinskega dela in uporabe informacijskih tehnologij za namen zagotavljanja kibernetske varnosti.
- Sposobnost fleksibilne uporabe pridobljenega znanja o kibernetski varnosti v praksi.

Predmetno-specifične kompetence:

- Sposobnost varnega in namenskega koriščenja najsodobnejših spletnih storitev.
- Napredno razumevanje varovanja informacij, ohranjanja njihove vrednosti in načinov zlorab informacij v realnem in kibernetskem prostoru.
- Seznanjenost s tehnologijami in načinom uporabe le te v informacijski družbi in potrebe ter vzroke za varovanje informacijskega premoženja.
- Obvladanje aktualnih mednarodnih standardov za zagotavljanje in evalvacijo sistemov za upravljanje z varnostjo informacij.

provide the basis for safe work in the real and cyberspace by reducing the misuse of information and privacy.

The instructional unit contributes to the development of the following general and subject-specific competences:
General competences:

- Understanding the importance of cyber security.
- The ability to identify cyber security risks and make proposals for action and protection based on identified risks.
- The ability to obtain, select, analyze information, as well as to interpret them to comprehensively solve problems, challenges and incidents in the field of cyber security.
- The ability to find data and sources for the needs of cyber security management.
- The ability to do business communication, teamwork and use of information technology to ensure cyber security.
- The ability of flexible usage of the acquired knowledge on cyber security in practice.

Subject-specific competences:

- Ability to safely and purposely utilize state-of-the-art online services
- Advanced understanding of information security, the preservation of their values and ways of misuse of the information in the physical world and cyberspace.
- Familiarity with the technology and how to use it in the information society and the needs and reasons for protecting information assets.
- Competence in current international standards for information security management system development and evaluation.

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: *Sposobnost študenta/študentke bo:* • razumeti celovit proces zagotavljanja varnosti v kibernetskem prostoru • uporabljati sodobne varnostne tehnologije za varno poslovanje v kibernetskem prostoru • analizirati stanje in oceniti varnostna tveganja • narediti varnostni načrt za celovito upravljanje kibernetske varnosti • upoštevati etične in pravne vidike za zagotavljanje skladnosti pri izvajanju kibernetsko varnostnih postopkov	Knowledge and understanding: The students will be able to: • understand the complex process of ensuring security in cyberspace • use of modern safety technologies for safe operation in the cyber space • analyze the situation and assess security risks • Make a safety plan for the overall management of cybersecurity • Work with the ethical and legal aspects to ensure consistency in the implementation of cyber security procedures

Metode poučevanja in učenja:	**Learning and teaching methods:**
• predavanja z aktivno udeležbo študentov (razlaga, diskusija, vprašanja, primeri, reševanje problemov) • laboratorijske vaje • individualne in skupinske konzultacije (diskusija, dodatna razlaga, obravnava specifičnih vprašanj)	• lectures with active participation of students (explanation, discussion, questions, examples, problem solving) • laboratory work • individual and group consultations (discussion, additional explanations and dealing with specific issues)

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt):		Type (examination, oral, coursework, project):
Pisni izpit	60 %	Written exam
Empirična seminarska naloga, poročila laboratorijskih vaj	40 %	Empirical seminar work, report on laboratory exercises

Reference nosilca / Lecturer's references:

- Bernik, I. (2014) Cybercrime and cyberwarfare, (Focus series). London: ISTE; Hoboken: Wiley.
- Tomažič, S., Bernik, I. (2019). Cyberattack response model for the nuclear regulator in Slovenia. *Journal of universal computer science*, ISSN 0948-6968, 2019, vol. 25, no. 11, str. 1437-1457.
- BERNIK, I. (2015). *Cybercrime : what we know about perpetrators*. V: Mileva Noshkoska, B. (ur.). Towards solving the social science challenges with computing methods. Frankfurt am Main: PL Academic Research. cop., str. 55-67.