UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Varnost posameznikov v kibernetskem prostoru
Course title:	Personal Cybersecurity

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	Prvi
The second cycle masters study programme Cyber Security	-	First	First

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

Predavanja **Lectures**	**Seminar** **Seminar**	**Vaje** **Tutorial**	**Klinične vaje** **work**	**Druge oblike študija**	**Samost. delo** **Individ. work**	**ECTS**
35	/	25	/	/	120	6

Nosilec predmeta / Lecturer:	prof. dr. Igor Bernik

Jeziki / Languages:	**Predavanja / Lectures:**	Slovenski / Angleški
	Vaje / Tutorial:	Slovenski / Angleški

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**
-	-

Vsebina:	Content (Syllabus outline):
• Posameznik, kibernetski prostor, kibernetska varnost. • (Ne)varnost storitev kibernetskega prostora. • Osebna varnost ali zasebnost? • Sodobna tehnologija v kibernetskem prostoru, uporaba in nevarnosti za uporabnike; osebnostni vidiki. • Upravljanje osebne identitete v kibernetskem prostoru. • Socialni inženiring. • Osebna skladnost s kibernetsko varnostjo. • Varovanje dostopa v kibernetski prostor. • Zavarovanje elektronskih podatkov posameznika – dostop, prenos, hranjenje. • Varovanje osebnega informacijskega premoženja. • Zavedanje in razumevanje tveganj, groženj in osebna obramba v kibernetskem prostoru. • Postopki ob zlorabah informacijskega premoženja v kibernetskem prostoru.	• The individual, cyberspace, cybersecurity. • (In)security of cyberspace services. • Personal security or privacy? • Modern technology in cyberspace, use and risks to users; the personal aspects. • Personal identity management in cyberspace. • Social engineering. • Personal compliance with cybersecurity. • Protecting access to cyberspace. • Securing individual data – access, transfer, storage. • Protection of electronic personal information assets. • Awareness and understanding of risks, threats, and personal defence in cyberspace. • Procedures in cases of abuse of information assets in cyberspace.

Temeljni literatura in viri / Readings:

- Waschke, M. (2017). Personal Cybersecurity: How to Avoid and Recover from Cybercrime, Apress, Združene države Amerike
- Mihelič, A., Jevšček, M., Vrhovec, S., Bernik, I. (2019) Testing the human backdoor: organizational response to a phishing campaign. Journal of universal computer science, 25 (11), str. 1458-1477
- Prislan, K., Mihelič, A., Bernik, I. (2020) A real-world information security performance assessment using a multidimensional socio-technical approach. PloS One, 15 (9), 17 str.

Cilji in kompetence:	Objectives and competences:
Splošne kompetence: • 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.	***General competences:*** • The ability to obtain, select, analyse 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.

• Sposobnost poslovnega komuniciranja, skupinskega dela in uporabe informacijskih tehnologij za namen zagotavljanja kibernetske varnosti. • Poznavanje pomena kakovosti in prizadevanje za kakovost strokovnega dela skozi avtonomnost, samoiniciativnost, (samo)kritičnost, (samo)refleksivnost in (samo)evalviranje. ***Predmetno-specifične kompetence:*** • Razumevanje pomena osebne kibernetske varnosti. • Sposobnost identifikacije kibernetskih varnostnih tveganj z vidika posameznika in izvedba zaščite na osnovi identificiranih tveganj. • Sposobnost fleksibilne uporabe pridobljenega znanja o kibernetski varnosti posameznika v praksi.	• The ability to do business communication, teamwork and use of information technology to ensure cyber security. • Knowledge of the importance of quality and striving for the quality of professional work through autonomy, self-initiative, as well as (self-)criticism, (self-)reflection and (self-)evaluation. ***Subject-specific competences:*** • Understanding the importance of personal cyber security. • The ability to identify cyber security risks and protection performance based on identified risks. • The ability of flexible usage of the acquired knowledge on cyber security in practice.
Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: *Študenti/študentke:* • Spoznajo ranljivosti komunikacije v kibernetskem prostoru z elektronskimi napravami in posledične grožnje, ki vodijo v kibernetsko varnostne dogodke oziroma incidente posameznika. • So zmožni razumeti varnostne ranljivosti kibernetskega prostora in elektronskih naprav in načine zlorab le-teh preko groženj. • Poznajo in razumejo namene in cilje upravljanja identitet, napadov s socialnim inženiringom in spoštovanja predpise s področja urejanja kibernetske varnosti. • Pridobijo zavedanje in razumevanje, kako se izogibati kibernetskim grožnjam ter kako zmanjšati vpliv tveganj in bolj varno delovati v kibernetskem prostoru z vzpostavitvijo osebne kibernetske obrambe. • So zmožni razumeti kibernetsko nesrečo in poznajo ter razumejo postopke obnove polnega delovanja dostopa do podatkov in naprav v	Knowledge and understanding: *Students:* • Understand the vulnerabilities of communications in the cyberspace with electronic devices and the consequent threats that lead to users' cybersecurity events or incidents. • They understand the security vulnerabilities of cyberspace and electronic devices and how they can be misused through threats. • Knows and understands the purposes and objectives of identity management, attacks with social engineering, and compliance with cybersecurity regulations. • Gain awareness and understanding of how to avoid cyber threats, how to reduce the impact of risks and operate more securely in cyberspace by establishing a personal cyber defence. • They understand a cyber disaster and understand the procedures for restoring the whole operation of cyber resilience after a cyber disaster.

kibernetskem prostoru po kibernetski nesreči.	

Metode poučevanja in učenja:	Learning and teaching methods:
• *predavanja* z aktivno udeležbo študentov (razlaga, diskusija, vprašanja, primeri, reševanje problemov) • *vaje na elektronskih napravah* • priprava seminarske naloge (funkcionalno pisanje, struktura, navajanje virov, obravnava specifičnih vprašanj)	• *lectures with active participation of students (explanation, discussion, questions, examples, problem solving* • *work on user's electronic devices* • *preparation of a seminar paper (functional writing, structure, citation of sources, discussion of specific issues)*

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt):		Type (examination, oral, coursework, project):
Pisni izpit	40	Written Exam
Seminarska naloga	20	Seminar work
Naloge na elektronskih napravah	40	Tasks on user’s electronic devices

Reference nosilca / Lecturer's references:

- Mihelič, A., Jevšček, M., Vrhovec, S., Bernik, I. (2019). Testing the human backdoor: organizational response to a phishing campaign. Journal of universal computer science, 25 (11), str. 1458-1477
- Prislan, K., Mihelič, A., Bernik, I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. PloS One, 15 (9), 17 str.
- Prislan, K., Bernik, I. (2020). Informacijska varnost in organizacije. 1. izd. Maribor: Univerzitetna založba Univerze; Ljubljana: Fakulteta za varnostne vede, 2019, 202 str.