

UČNI NAČRT PREDMETA / COURSE SYLLABUS

Predmet:	Varnost posameznikov v kibernetnem prostoru
Course title:	Personal Cyber Security

Študijski program in stopnja	Študijska smer	Letnik	Semester
Study programme and level	Study field	Academic year	Semester

Kibernetna 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-2026-01-28

Predavanja Lectures	Seminar Seminar	Vaje Tutorial	Klinične vaje work	Druge oblike študija	Samost. delo Individ. work	ECTS
20	/	20	/	/	140	6

Nosilec predmeta / Lecturer:

prof. dr. Igor Bernik

Jeziki / Predavanja / Lectures:

Slovenski / Angleški

Languages: Vaje / Tutorial:

Slovenski / Angleški

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:

-

Prerequisites:

-

Vsebina:

- Posameznik, kibernetški prostor, kibernetška varnost.
- (Ne)varnost storitev kibernetškega prostora.
- Osebna varnost ali zasebnost?
- Sodobna tehnologija v kibernetškem prostoru, uporaba in nevarnosti za uporabnike; osebni vidiki.
- Upravljanje osebne identitete v kibernetškem prostoru.
- Socialni inženiring.
- Osebna skladnost s kibernetško varnostjo.
- Varovanje dostopa v kibernetški prostor.
- Zavarovanje elektronskih podatkov posameznika – dostop, prenos, hranjenje.
- Varovanje osebnega informacijskega premoženja.
- Zavedanje in razumevanje tveganj, groženj in osebna obramba v kibernetškem prostoru.
- Postopki ob zlorabah informacijskega premoženja v kibernetškem prostoru.

Content (Syllabus outline):

- The individual, cyberspace, cyber security.
- (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 cyber security.
- 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.

Temeljna 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
- Prislán, 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.
- Khan, N., Ahmad, K., Al Tamimi, A., Alani, M.M., Bermak, A., & Khalil, I. (2025). *Explainable AI-Based Intrusion Detection Systems for Industry 5.0 and Adversarial XAI: A Systematic Review*.
- Mohamed, N. (2025). *Artificial intelligence and machine learning in cybersecurity*.
- Muneer, et al. (2024). *A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis*.
- VRHOVEC, Simon, BERNIK, Igor, MARKELJ, Blaž. Explaining information seeking intentions. *Computers & security*. [Print ed.]. Feb 2023, vol. 125, art. 103038

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 kibernetске varnosti.
- Sposobnost iskanja podatkov in virov za potrebe upravljanja kibernetске varnosti.
- Sposobnost poslovnega komuniciranja, skupinskega dela in uporabe informacijskih tehnologij za namen zagotavljanja kibernetске 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 kibernetске varnosti.
- Sposobnost identifikacije kibernetских varnostnih tveganj z vidika posameznika in izvedba zaščite na osnovi identificiranih tveganj.
- Sposobnost fleksibilne uporabe pridobljenega znanja o kibernetски varnosti posameznika v praksi.

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.
- 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:

Znanje in razumevanje:

Študenti/študentke:

- Spoznajo ranljivosti komunikacije v kibernetskem prostoru z elektronskimi napravami in posledične grožnje, ki vodijo v kibernetско 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 kibernetске varnosti.
- Pridobijo zavedanje in razumevanje, kako se izogibati kibernetским

Intended learning outcomes:

Knowledge and understanding:

Students:

- Understand the vulnerabilities of communications in the cyberspace with electronic devices and the consequent threats that lead to users' cyber security 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 cyber security regulations.
- Gain awareness and understanding of how to avoid cyber threats, how to reduce the impact of risks and operate

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 kibernetskem prostoru po kibernetski nesreči.

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.

Metode poučevanja in učenja:

- predavanja z aktivno udeležbo študentov (razlaga, diskusija, vprašanja, primeri, reševanje problemov)
- laboratorijske vaje
- individualne in skupinske konzultacije (diskusija, dodatna razlaga, obravnava specifičnih vprašanj)

Learning and teaching methods:

- 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)

Delež (v %) /

Načini ocenjevanja:

Weight (in %) **Assessment:**

Način (pisni izpit, ustno izpraševanje, naloge, projekt):		Type (examination, oral, coursework, project):
Pisni izpit	60	Written exam
Empirična seminarska naloga in poročila laboratorijskih vaj	40	Empirical seminar work and report on laboratory exercises

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
- Prislán, 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.
- Prislán, K., Bernik, I. (2020). *Informacijska varnost in organizacije*. 1. izd. Maribor: Univerzitetna založba Univerze; Ljubljana: Fakulteta za varnostne vede, 2019, 202 str.
- VRHOVEC, Simon, BERNIK, Igor, MARKELJ, Blaž. Explaining information seeking intentions. *Computers & security*. [Print ed.]. Feb 2023, vol. 125, art. 103038
- BERNIK, Igor. Izzivi informacijske varnosti pri prehodu v družbo 5.0. V: MARKELJ, Blaž (ur.). *Informacijska varnost: doba tehnoloških prebojev in pravnih izzivov*. 1. natis. Ljubljana: Lexpera, GV Založba, 2023. Str. 13-34, 169.