UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Varnost organizacij
Course title:	Organizations' 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
The second cycle masters study programme Cyber Security	-	First	Second

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

Predavanja Lectures	Seminar Seminar	Vaje Tutorial	Klinične vaje work	Druge oblike študija	Samost. delo Individ. work	ECTS
25	-	15	-	-	80	4

Nosilec predmeta / Lecturer:	doc. dr. Boštjan Delak
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:
Za vključitev v delo je potrebo usvojiti zanje predmetov Pravo informacijske varnosti, Varnost omrežij, Varnost posameznikov v kibernetskem prostoru, Varnosti in zavarovanje podatkov in Varnost sistemov. Študent/študentka mora pred pristopom k izpitu pripraviti in zagovarjati seminarsko nalogo.	In order to be included in the work, it is necessary to master the content of the following courses: Information Security Law, Network Security, Personal Cybersecurity, Data security and protection, and System security. Prior to the exam, the student has to prepare and present seminar work.

Vsebina:	Content (Syllabus outline):
• Tveganja: analiza in upravljanje s tveganji; informacijska tveganja, okoljski vplivi. • Upravljanje informacijske varnosti: strateški, taktični in operatvoni management, dimenzije upravljanja.	• Risks: Risk analysis and management; information risks, environmental impacts. • Information security management: Strategic, tactical and operational management, management dimensions.

• Uspešnost in učinkovitost informacijske varnosti: Elementi kakovosti varnosti, razmerje med funkcionalnostjo in varnostjo informacijskih sistemov. • Ukrepi informacijske varnosti: Kontrole, standardi, okvirji in metodologije za upravljanje informacijske varnosti. • Organizacijski informacijsko varnostni ukrepi: varnostni management, varnostna strategija in politika informacijske varnosti, skladnost z zakonodajo, upravljanje kadrovskih virov, varnostna kultura in ozaveščenost uporabnikov, upravljanje odnosov z zunanjimi subjekti. • Tehnični ukrepi: Ukrepi fizične varnosti, ukrepi tehničnega varovanje informacijske varnosti. • Neprekinjeno poslovanje: strategija, politika, načrti neprekinjenega poslovanja, krizno obveščanje, načrti okrevanja, testiranje, analiza, izboljševanje.	• Effectiveness and efficiency of information security: Elements of security quality, the relationship between functionality and security of information systems. • Information security measures: Controls, standards, frameworks and methodologies for information security management. • Organizational information security measures: Security management, security strategy and information security policy, compliance with legislation, human resources management, security culture and user awareness, management of relations with external entities. • Technical measures: Physical security measures, technical security measures of information security. • Business continuity: Strategy, policy, business continuity plans, crisis information, recovery plans, testing, analysis, improvements.

Temeljni literatura in viri / Readings:

- Kaja Prislan, Igor Bernik, *Informacijska varnost in organizacije,* Univerza v Mariboru, Fakulteta za varnostne vede, 2019.
- Isabella Corradini, *Building a Cybersecurity Culture in Organization,* Springer, 2020.
- Ariel Evens, *Enterprise Cybersecurity in Digital Business – Building a Cyber Resilient Organization,* Routledge, 2021.

Cilji in kompetence:	**Objectives and competences:**
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 iskanja podatkov in virov za potrebe upravljanja kibernetske varnosti.	*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 find data and sources for the needs of cyber security management. • The ability to do business communication, teamwork and use

• sposobnost poslovnega komuniciranja, skupinskega dela in uporabe informacijskih tehnologij za namen zagotavljanja kibernetske varnosti. • sposobnost razvoja informacijskih varnostnih politik in sistemov upravljanja organizacije. ***Predmetno-specifične kompetence***: • sposobnost identificirati kibernetska tveganja organizacije, • sposobnost izvajati upravljanje informacijske varnosti, • sposobnost preverjanja ustreznosti implementiranih kontrol kibernetske varnosti, • sposobnost priprave in nadgradnje strategij, politik in drugih internih aktov na področju kibernetske varnosti • sposobnost upravljanja sistema neprekinjenega poslovanja organizacije.	of information technology to ensure cyber security. • The ability to develop information security policies and management systems of the organization. ***Subject-specific competences:*** • The ability to identify the organization's cyber risks, • The ability to perform information security management, • The ability to check the adequacy of implemented cyber security controls, • The ability to prepare and upgrade strategies, policies and other internal acts in the field of cyber security • The ability to manage the business continuity system within organization.

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: *Sposobnost študenta/študentke bo:* • znal identificirati in analizirati tveganja ter predlagati vpeljavo ukrepov / kontrol za zmanjšanje tveganj na področju kibernetske varnosti • ustrezno razmejiti upravljanje varnosti na različnih področjih in upravljati različne dimenzije varnosti organizacije • prepoznaval elemente kakovosti varnosti in jih znal odločati med funkcionalnostjo in varnostjo • znal izbrati ustrezne ukrepe in kontrole za zmanjševanje ranljivosti organizacije • ustrezno pripraviti strategijo, politike in pripadajoče dokumente na področju informacijske varnosti • uspešno upravljati neprekinjeno poslovanje organizacije s	Knowledge and understanding: The ability of the students will be: • be able to identify and analyze risks and propose the introduction of measures / controls to reduce risks in the field of cyber security • appropriately delineate security management in different areas and apply different dimensions of organisational security • recognize the elements of safety quality and know how to decide between functionality and safety • be able to choose appropriate measures and controls to reduce the vulnerability of the organization • appropriate preparation of strategy, policies and related documents in the field of information security • successfully manage the business continuity of the organization with the corresponding intensive plans, documents and measures.

pripadajočimi internimi načrti, dokumenti in ukrepi.	

Metode poučevanja in učenja:	**Learning and teaching methods:**
• *predavanja* z aktivno udeležbo študentov (razlaga, diskusija, vprašanja, primeri, reševanje problemov) • vaje z izdelavo domačih nalog in izdelava seminarske naloge • individualne in skupinske konzultacije (diskusija, dodatna razlaga, obravnava specifičnih vprašanj)	• *lectures with active participation of students (explanation, discussion, questions, examples, problem solving* • *exercises with homework and seminar work* • *individual and group consultations (discussion, additional explanation deals 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
• priprava in zagovor seminarske naloge,	30	• preparation and presentation of seminar work
• domače naloge	10	• homework

Reference nosilca / Lecturer's references:

- DREV, Matjaž, DELAK, Boštjan. Conceptual Model of Privacy by Design. Journal of computer information systems. 2021, vol. , iss. , str. 1-8, ilustr. ISSN 0887-4417. DOI: 10.1080/08874417.2021.1939197. [COBISS.SI-ID 74349827].
- KAVČIČ, Tina, DELAK, Boštjan. State of the cyber insurance products within Slovenian insurance companies. The Online journal of applied knowledge management. 2019, vol. 7, iss. 2, str. 56-68, tabele. ISSN 2325-4688. [COBISS.SI-ID 44763651].
- DELAK, Boštjan. Revizija neprekinjenega poslovanja = Business continuity audit. Sir*ius : revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij. 2019, št. 5, str. 3-17. ISSN 2335-3252. http://www.si-revizija.si/publikacijesirius/kazala-letnikov. [COBISS.SI-ID 2048620563].
- DAVIS, Keiona, LEVY, Yair, DELAK, Boštjan. Towards a development of cybersecurity risk-responsibility taxonomy of small enterprises for data breach mitigation. V: Digital disruption. 24th Americas Conference on Information Systems (AMCIS), New Orleans, LA, August 16-18, 2018. [S. l.]: Association for Information Systems, 2018. Str. 1-6. ISBN 978-0-9966831-6-6- https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1338&context=amcis2018, https://aisel.aisnet.org/amcis2018/Security/Presentations/8/. [COBISS.SI-ID 2048569363].
- DELAK, Boštjan. Izzivi revizorjev informacijskih sistemov pri dajanju zagotovil pri logičnih dostopih = The information systems auditors' issues at the logical access audit assurance activities. Sir*ius : revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij. sep. 2016, let. 4, št. 5, str. 5-27, graf. prikazi, tabele. ISSN 2335-3252. [COBISS.SI-ID 23241958].

- DELAK, Boštjan. Approach for information system maturity assessment. V: KARAGIANNIS, Dimitris (ur.), SCHLAMBERGER, Niko (ur.). Proceedings of the CAiSE 2016 Industry Track co-located with 28th International Conference on Advanced Information Systems Engineering (CAiSE 2016), Ljubljana, Slovenia, June 13-17, 2016, (CEUR workshop proceedings, ISSN 1613-0073, Vol. 1600). [S. l.]: CEUR-WS. 2016, str. 1-15.