UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Varnost in zavarovanje podatkov
Course title:	Data security and protection

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-VZP-2021-12-14

Predavanja **Lectures**	**Seminar** **Seminar**	**Vaje** **Tutorial**	**Klinične vaje** **work**	**Druge oblike študija**	**Samost. delo** **Individ. work**	**ECTS**
40	/	20	/	/	120	6

Nosilec predmeta / Lecturer:	doc. dr. Igor Tomičić

Jeziki / **Languages:**	**Predavanja / Lectures:**	Slovenski, angleški / Slovene, English
	Vaje / Tutorial:	Slovenski, angleški / Slovene, English

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

Za vključitev v delo je potrebno, da se študent seznani z osnovnimi kriptografskimi termini. Za pristop k izpitu mora študent pripraviti in predstaviti projektno nalogo.	It is required for a student to be familiar with basic cryptography terms. To attend the exam, a student has to prepare and present a project assignment.

Vsebina:	**Content (Syllabus outline):**
• Klasifikacija podatkov in povezana tveganja • Viri podatkov, vrste shranjevanja • Elementi sistema varstva podatkov • Uporabna kriptografija • Kontrole dostopa do podatkov • Varnostno kopiranje podatkov, obnovitev, arhivi • Odpravljanje podvajanja • Metode obnovitve po nesreči • Varnost podatkov v neprekinjenem poslovanju • Zaščita baz podatkov • Tradicionalne in sodobne rešitve za varstvo podatkov • Varnostni vidiki podatkov v oblaku • Varnostni vidiki velikih podatkov • Zasebnost in pravni vidiki varstva podatkov	• Data classification and associated risks • Data sources, storage types • Elements of data protection system • Applied cryptography • Data Access controls • Data backup, recovery, archives • Deduplication • Disaster recovery methods • Data security in business continuity • The protection of databases • Traditional and modern data protection solutions • Security aspects of Data in Cloud • Security aspects of Big Data • Privacy and legal considerations of data protection

Temeljni literatura in viri / Readings:

- Preston, W. C. (2021). *Modern Data Protection: Ensuring Recoverability of All Modern Workloads*. O'Reilly Media.
- De Guise, P. (2020). *Data protection: Ensuring data availability* (2nd ed.). Auerbach Publications.
- Yang, P., Xiong, N., & Ren, J. (2020). *Data security and privacy protection for cloud storage: A survey*. IEEE Access, 8, 131723-131740.
- Alsulbi, K., Khemakhem, M., Basuhail, A., Eassa, F., Jambi, K. M., & Almarhabi, K. (2021). *Big Data Security and Privacy: A Taxonomy with Some HPC and Blockchain Perspectives.* International Journal of Computer Science & Network Security, 21(7), 43-55.
- Tomičić, I. *Prosojnice iz predavanj in vaj pri predmetu Varnost in zavarovanje podatkov.* Moodle FIŠ.

Cilji in kompetence:	**Objectives and competences:**

Splošne kompetence:	***General competences:***
• Razumevanje pomena kibernetske varnosti. • Poznavanje pravnih in etičnih vidikov varovanja podatkov in informacij. • Sposobnost fleksibilne uporabe pridobljenega znanja o kibernetski varnosti v praksi.	• Understanding the importance of cyber security. • Knowledge of legal and ethical aspects of data and information protection. • Ability to flexibly apply the acquired knowledge of cyber security in practice.
Predmetno-specifične kompetence:	***Subject-specific competences:***
• Sposobnost razločevanja in kategorizacije različnih vrst podatkov, ki jih najdemo v organizaciji. • Razumevanje možnih ranljivosti in tveganj za varnost podatkov. • Sposobnost uporabe učinkovitih kripto sistemov v različnih primerih uporabe. • Razumevanje elementov sistema varstva podatkov. • Sposobnost izvajanja učinkovitih sistemov za varnostno kopiranje, obnovitev in arhiviranje. • Sposobnost predlaganja učinkovitih sistemov za nadzor dostopa do podatkov. • Razumevanje pomena deduplikacije. • Sposobnost uporabe ustreznih metod zaščite baze podatkov. • Razumevanje neprekinjenega poslovanja, zasebnosti in pravnih vidikov v kontekstu varstva podatkov. • Sposobnost prepoznavanja in argumentiranja o možnostih, priložnostih in tveganjih podatkov v oblaku.	• Ability to discern and categorize various data types found in an organization. • Understanding of potential vulnerabilities and risks to data security. • Ability to apply effective crypto systems to various use-cases. • Understanding of elements of data protection system. • Ability to implement effective backup, recovery and archive systems. • Ability to propose effective data access control systems. • Understanding of the significance of deduplication. • Ability to apply appropriate database protection methods. • Understanding of business continuity, privacy and legal considerations in the context of data protection. • Ability to recognize and argue about the possibilities, opportunities and risks of data in cloud.

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: • Študentje se bodo seznanili s teoretičnimi osnovami in praktičnimi navodili glede sodobnih vidikov varnosti in zaščite podatkov. • Študentje bodo znali uporabiti nekatere sodobne elemente varnosti podatkov (šifriranje, metode varnostnega kopiranja / obnovitve, metode zaščite	Knowledge and understanding: • The students will get acquainted with theoretical basics and practical instructions on modern data security and protection aspects. • Students will be able to apply some of the modern data security elements (encryption, backup/restore methods, database protection methods, etc.) to various use-cases.

baze podatkov itd.) v različnih primerih uporabe. • Študenti se bodo lahko pogovarjali in predlagali metode varnosti in zaščite podatkov v okviru neprekinjenega poslovanja. • Študentje se bodo lahko pogovarjali o varnostnih vidikih velikih podatkov in podatkov v oblaku ter o zasebnosti in pravnih vidikih varstva podatkov.	• Students will be able to argue about and propose data security and protection methods in the context of business continuity. • Students will be able to argue about security apsects of big data and data in cloud, as well as privacy and legal aspects of data protection.

Metode poučevanja in učenja:	**Learning and teaching methods:**
• *Predavanja* z aktivnim sodelovanjem študentov (razlaga, razprava, vprašanja, primeri); • *Vaje*, na katerih bodo študenti uporabljali različna orodja in sisteme za reševanje danih vaj (npr. Gpg4win, certutil, VeraCrypt, CrypTool, Cain&Abel, virtualni stroji, različne spletne storitve); • *Vaje*, na katerih bodo študenti predstavili rezultate svojih projektov in vključili vse udeležence v konstruktivno razpravo in predhodno ocenjevanje.	• *Lectures with active participations by the students* (explanation, discussion, questions, cases); • *Tutorials*, where students will use various tools and systems to solve given exercises (for example Gpg4win, certutil, VeraCrypt, CrypTool, Cain&Abel, virtual machines, various online services); • *Tutorials,* where students will present the results of their projects and include all participants in a constructive discussion and preliminary assessment.

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Projektna naloga	40 %	Project assignment
Pisni izpit	60 %	Written Exam

Reference nosilca / Lecturer's references:

- Tomičić, Igor; Grd, Petra. Towards the open ontology for IoT ecosystem's security // MIPRO 2020 43rd International Convention Proceedings / Skala, Karolj (ur.). Rijeka: Croatian Society for Information, Communication and Electronic Technology – MIPRO, 2020. str. 1308-1313.
- Tomičić, Igor; Peharda, Tomislav; Bernik, Andrija. An Active Game Bot Detection with Security Bots // Central European Conference on Information and Intelligent Systems Varaždin, 2021. str. 25-31.
- Grd, Petra; Tomičić, Igor; Bača, Miroslav. Privacy improvement model for biometric person recognition in ambient intelligence using perceptual hashing // Proceedings of the Central European Cybersecurity Conference 2018.
- Cindori, Dominik; Tomičić, Igor; Grd, Petra. Security Hardening of Facial Recognition Systems // Proceedings - 44th International Convention on Information, Communication and Electronic Technology / Karolj, Skala (ur.). Rijeka: Croatian

Society for Information, Communication and Electronic Technology – MIPRO, 2021. str. 1176-1180.
- Viktorovych Shkarupylo, Vadym; Tomičić, Igor; Mykolaiovych Kasian, Kostiantyn; Abedalrahim Jamil Alsayaydeh, Jamil. An approach to increase the effectiveness of tlc verification with respect to the concurrent structure of tla+ specification // International Journal of Software Engineering and Computer Systems, 4 (2018), 1; 48-60 doi:10.15282/ijsecs.4.1.2018.4.0037.