UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Umetna inteligenca
Course title:	Artificial Intelligence

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	Izbirni / Elective
Univerzitetna koda predmeta / University course code:	5-KV-MAG-IP-UI-2021-12-14

Predavanja **Lectures**	**Seminar** **Seminar**	**Vaje** **Tutorial**	**Klinične vaje** **work**	**Druge oblike študija**	**Samost. delo** **Individ. work**	**ECTS**
30	/	30	/	/	90	5

Nosilec predmeta / Lecturer:	doc. dr. Panče Panov

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

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**
Za vključitev v delo je potrebno osnovno znanje iz matematike, programiranja in podatkovnih baz. Pogoj za pristop k izpitu je priprava in zagovor projektne naloge.	Basic knowledge of maths, programming and databases is required. To attend the exam, a student has to prepare and present a project assignment.

Vsebina:	**Content (Syllabus outline):**
• Uvod v umetno inteligenco (kaj je umetna inteligenca?, temelji, zgodovina, sodobni razvoj področja) • Inteligentni agenti (agenti in okolje, narava okolja, struktura agentov) • Reševanje problemov (reševanje problemov z preiskovanjem, preiskovanje v kompleksnem okolju, igre) • Znanje, sklepanje in načrtovanje (predstavljanje znanja z logiko, ontologije, logično sklepanje, avtomatsko načrtovanje) • Strojno učenje (učenje iz primerov, nadzorovano učenje, simbolično učenje, učenje numeričnih modelov, globoko učenje, ansambli modelov, izbira modelov in optimizacija, nenadzorovano učenje, spodbujevalno učenje, razvoj sistemov za strojno učenje) • Obdelava naravnega jezika (jezikovni modeli, korpusi besedil, vložitve besed in globoko učenje za naloge obdelave naravnega jezika) • Računalniški vid (uvod, ustvarjanje slik, značilke slik, klasifikacija slik, detekcija objektov) • Primeri uporabe umetne inteligence za reševanje problemov kibernetske varnosti (odkrivanje novih groženj, boj z boti, napovedovanje tveganja nedovoljenega vstopanja, izboljšana zaščita končnih točk)	• Introduction to artificial intelligence (what is AI?, foundations of AI, history of AI, state-of—the-art developments) • Intelligent agents (agents and environment, nature of environments, structure of agents) • Problem-solving (Problem solving by searching, search in complex environments, games) • Knowledge, reasoning and planning (knowledge representation with logics, ontologies, logical inference, automatic planning) • Machine learning (learning from examples, supervised learning, symbolic learning, learning numerical models, deep learning, ensembles of models, model selection and optimization, unsupervised learning, reinforcement learning, design and development of machine learning systems) • Natural language processing (language models, language corpora, word embedings and deep learning for natural language processing) • Computer vision (introduction, formation of images, image features, image classification, object detection) • Examples of use of artificial intelligence for solving cyber security problems (detection of new threats, battling bots, breach risk prediction, improved endpoint protection)

Temeljni literatura in viri / Readings:

- Russell, S., Norvig, P. (2021) Artificial Intelligence – A Modern Approach (4 th edition). Pearson.
- Aggarwal, C. (2021) Artificial Intelligence – A Texbook. Springer.
- Moroney, L. (2020) AI and Machine Learning for Coders. O' Reilly Media, Inc.
- Sikos, L. (ed) (2019) AI in Cybersecurity. Springer.
- Parisi. A (2019) Hands-On Artificial Intelligence for Cybersecurity. Packt.
- Kononenko, I., Robnik Šikonja, M. (2010) Inteligentni sistemi. Založba FE in FRI.
- Bratko, I. (2011) Prolog in umetna inteligenca. Založba FE in FRI.

Cilji in kompetence:

Splošne kompetence:

- Sposobnost uporabe različnih programskih rešitev za zagotavljanje, upravljanje, nadzorovanje in evalvacijo kibernetske varnosti.
- Sposobnost fleksibilne uporabe pridobljenega znanja o kibernetski varnosti v praksi.

Predmetno-specifične kompetence:

- sposobnost reševanja problemov v umetni inteligenci s tehnikami preiskovanja,
- sposobnost predstavljanja domenskega znanja v formalnem jeziku logike,
- sposobnost uporabe metod strojnega učenja ter obdelave naravnega jezika za reševanje problemov iz kibernetske varnosti,
- sposobnost uporabe tehnik računalniškega vida za reševanje problemov kibernetske varnosti,
- sposobnost načrtovanja uporabe ustreznih metod umetne inteligence pri reševanju problemov v praksi.

Objectives and competences:

General competences:

- The ability to use various software solutions to provide, manage, monitor and evaluate cyber security.
- The ability of flexible usage of the acquired knowledge on cyber security in practice.

Subject-specific competences:

- Ability to solve problems in artificial intelligence by using search techniques,
- Ability to represent knowledge in a formal logical language,
- Ability to use machine learning methods and natural language processing for solving cybersecurity problems,
- Ability to use computer vision techniques for solving cybersecurity problems,
- Ability to design and use adequate AI methods for solving practical problems

Predvideni študijski rezultati:

Intended learning outcomes:

Znanje in razumevanje:	Knowledge and understanding:
• študenti bodo spoznali temeljne koncepte umetne inteligence ter sodobne smeri, v katerih se področje razvija; • študenti se bodo seznanili s konceptom inteligentnega agenta ter strukturo agentov in pomena okolja, v katerem agent deluje; • študenti bodo spoznali različne načine reševanja problemov v umetni inteligenci s pomočjo tehnik preiskovanja; • študenti se bodo seznanili s pomenom predstavljanja znanja v formalnem jeziku ter konceptom avtomatičnega sklepanja in načrtovanja dejanj inteligentnih agentov; • študenti se bodo spoznali z osnovnimi koncepti, nalogami in metodami iz strojnega učenje ter bodo sposobni uporabiti to znanje v konkretnih primerih v področju kibernetske varnosti; • študenti se bodo spoznali z različnimi metodami obdelave naravnega jezika; • študenti se bodo spoznali z osnovnimi koncepti iz računalniškega vida ter nalogami, ki so pomembne v kontekstu kibernetske varnosti kot so ekstrakcija značilk iz slik, klasifikacija slik ter avtomatska detekcija objektov; • Študenti bodo seznanjeni z prototipnimi primeri uporabe umetne inteligence za reševanje problemov kibernetske varnosti in bojo sposobni načrtovati in uporabiti metode umetne inteligence pri svojem delu na področju.	• The students will be acquainted with the basic concepts of AI and the state-of-the-art developments in the field; • The students will be knowledgeable of the intelligent agent concept as well as the structure of agents and the importance of the environment, in which the agent acts; • The students will learn how to use different search techniques to solve problems in AI; • The students will be acquainted with representing knowledge in a formal language and the concepts of automatic reasoning and planning; • The students will be knowledgeable of basic concepts, tasks and methods from machine learning and will be able to use the knowledge for solving concrete problems in the area of cybersecurity; • The students will be knowledgeable of different methods for natural language processing; • The students will be able to use the basic methods from computer vision, such as feature extraction, image classification and object detection for solving problems in cybersecurity; • The students will be knowledgeable of the prototypic problems from cybersecurity that can be solved by using AI and will be able to use that knowledge to design and implement AI methods in their work in the area.

Metode poučevanja in učenja:	**Learning and teaching methods:**
• *Predavanja z aktivno udeležbo študentov* (razlaga, diskusija, vprašanja, primeri, reševanje problemov); • *Vaje*, kjer študentje na primerih ponovijo temeljne koncepte, predstavljene na predavanjih; • *Laboratorijske vaje*, kjer se študenti naučijo uporabljati različne programske	• *Lectures with active participations by the students* (explanation, discussion, questions, cases, problems solving); • *Tutorials*, where students will recall, reinforce, and shed light on the concepts and methods introduced at lectures;

knjižnice, ki implementirajo različne algoritme iz umetne inteligence.	• *Lab work*, where students will learn to use to use different libraries that implement AI algorithms.

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt):		Type (examination, oral, coursework, project):
Pisni izpit	60 %	Written Exam
Projektna naloga	40 %	Project assignment

Reference nosilca / Lecturer's references:

- Osojnik, A., Panov, P., Džeroski, S. (2020) Incremental predictive clustering trees for online semi-supervised multi-target regression. Machine learning vol. 109, no. 11, str. 2121-2139 [COBISS.SI-ID 37128707]
- Tolovski, I., Džeroski, S., Panov, P. (2020). Semantic annotation of predictive modelling experiments. In: Proceedings of 23rd International Conference on Discovery Science, DS 2020, Thessaloniki, Greece, October 19-21, 2020, *Lecture notes in computer science Vol. 12323*, 124-139 [COBISS.SI-ID 37131267]
- Kostovska, A., Džeroski, S., Panov, P. (2020). Semantic description of data mining datasets: an ontology-based annotation schema. In: Proceedings of 23rd International Conference on Discovery Science, DS 2020, Thessaloniki, Greece, October 19-21, 2020, *Lecture notes in computer science Vol. 12323*, 140-155. [COBISS.SI-ID 37133315]
- Kostovska, A., Tolovski, I., Maikore, F., Soldatova, L., Panov, P. (2019). Neurodegenerative disease data ontology, In: Proceedings of 22nd International Conference on Discovery Science DS 2019, Split, Croatia, October 28-30, 2019, *Lecture notes in computer science Vol. 11828*, 235-245. [COBISS.SI-ID 32864807]
- Tolovski, I., Kostovska, A., Simidjievski, N., Todorovski, L., Džeroski, S., Panov, P. (2019) Towards reusable process-based models of dynamical systems : a case study in the domain of aquatic ecosystems, In: Proceedings of 42nd International Convention MIPRO 2019, May 20 -24, 2019, Opatija, Croatia, pp. 1110-1115. [COBISS.SI-ID 32541991]
- Osojnik, A., Panov, P., Džeroski, S. (2018) Tree-based methods for online multi-target regression. Journal of intelligent information systems vol. 50, no. 2, str. 315-339 [COBISS.SI-ID 30463783
- Osojnik, A., Panov, P., Džeroski, S. (2017) Multi-label classification via multi-target regression on data streams. Machine learning, ISSN 0885-6125. [Print ed.], 2017, vol. 106, no. 6, str. 745-770, doi: 10.1007/s10994-016-5613-5. [COBISS.SI-ID 30119463]
- Lawrynowicz, A., Esteves, D., Panov, P., Soru, T., Džeroski, S., Vanschoren, J. (2017) An algorithm, implementation and execution ontology design pattern. *Studies on the semantic web, vol. 32*, 55-68, IOS Press. [COBISS.SI-ID 31363623]

- Panov, P., Soldatova, L., Džeroski, S.(2016) Generic ontology of datatypes, *Information sciences, vol. 329*, 900-920. [COBISS.SI-ID 28796199]
- Soldatova, L., Panov, P., Džeroski, S. (2015) Ontology engineering : from an art to a craft, In: 12th International Experiences and Directions Workshop on OW, OWLED, 2015 revised and selected papers, *Lecture notes in computer science, vol. 9557*, 174-181. [COBISS.SI-ID 29448231]
- Panov, P., Soldatova, L., Džeroski, S. (2014) Ontology of core data mining entities, *Data mining and knowledge discovery, Vol. 28, no. 5/6*, 1222-1265. [COBISS.SI-ID 27814439]
- Panov, P., Soldatova, L., Džeroski, S. (2013) OntoDM-KDD: ontology for representing the knowledge discovery process", In: Proceedings of 16th International Conference on Discovery Science, DS 2013, Singapore, October 6-9, 2013. *Lecture notes in computer science vol. 8140*, 126-140. [COBISS.SI-ID 27143207]