UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Kibernetska varnost interneta stvari in operativnih tehnologij
Course title:	Internet of things and operational technologies 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	-	Drugi	Tretji
The second cycle masters study programme Kibernetska varnost	-	Second	Third

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

Predavanja **Lectures**	**Seminar** **Seminar**	**Vaje** **Tutorial**	**Klinične vaje** **work**	**Druge oblike študija**	**Samost. delo** **Individ. work**	**ECTS**
30	/	30	/	/	120	6

Nosilec predmeta / Lecturer:	red. prof. dr. Andrej Škraba

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 poznavanje principov razvoja algoritmov in podatkovnih struktur ter usvojene vsebine predmetov Varnost omrežij, Varnost sistemov, Varnost komponent in Varnost in zavarovanje podatkov.	In order to participate in the course, the basic knowledge of algorithms and data structures development is needed, and to master the content of the following courses: Network Security, Data security and protection, System security, and Component Security.

Vsebina:	**Content (Syllabus outline):**
• Internet stvari s primeri aplikacij, strojna in programska oprema • Operativne tehnologije s primeri aplikacij, strojna in programska oprema • Nadzorni sistemi operativnih tehnologij in zajem podatkov • Distribuirani kontrolni sistemi operativnih tehnologij • Varnostni vidiki povezave z oblačnimi informacijskimi sistemi • Varnostni protokoli interneta stvari in operativnih tehnologij • Cilji zagotavljanja kibernetske varnosti interneta stvari ter operativnih tehnologij • Hierarhija industrijskih kontrolnih sistemov • Standardi kibernetske varnosti na področju interneta stvari ter operativnih tehnologij • Identifikacija ranljivosti sistemov operativnih tehnologij ter interneta stvari • Varnost robnih naprav in storitvenih platform • Varnost podpornih poslovnih informacijskih sistemov v povezavi z internetom stvari in operativnimi tehnologijami • Identifikacija kibernetskih groženj in možnih posledic • Pregled znanih napadov na kritično infrastrukturo na področju interneta stvari in operativnih tehnologij • Spremljanje omrežnih aktivnosti, identifikacija groženj • Varnostni dnevnik in podatkovna analitika za identifikacijo varnostnih groženj • Modeliranje varnostnih kibernetskih groženj	• Internet of things with practical example, hardware and software considerations • Operational technology with practical example, hardware and software considerations • Operational technology supervision, control and data acquisition • Distributed control systems of operational technology • Security consideration of cloud-based information systems interconnections • Security protocols of operational technologies and internet of things • Goals of operational technologies and internet of things cybersecurity • Hierarchy of industrial control systems • Standards of cybersecurity in the field of internet of things and operational technology • Identification of key vulnerabilities of operational technologies and internet of things • Security of edge devices and Platforms-as-a-Service – PaaS • Security of enterprise support backend applications connected to operational technologies and internet of things • Identification of cyber threats and possible consequences • Overview of known attacks on critical infrastructure in the field of operational technologies and internet of things • Network monitoring, threats identification • Security log and data analytics to identify cybersecurity threats • Modelling of cybersecurity threats • Organization of the system to provide cybersecurity of operational technologies and internet of things

• Organiziranje sistema za zagotavljanje kibernetske varnosti interneta stvari ter operativnih tehnologij • Zadolžitve ekipe za zagotavljanje kibernetske varnosti interneta stvari in operativnih tehnologij • Predvidevanje varnostnih groženj in raziskave na področju interneta stvari in operativnih tehnologij	• Cybersecurity action team tasks to protect operational technologies and internet of things • Anticipation of cybersecurity threats and research in the field of operational technologies and internet of things

Temeljni literatura in viri / Readings:

- Shiaeles S. (ur.), N. Kolokotronis (ur.) (2021) Internet of Things, Threats, Landscape, and Countermeasures, CRC Press
- Colbert E. . M. (ur.), A. Kott (ur.) (2016) Cyber-security of SCADA and Other Industrial Control Systems (Advances in Information Security Book 66), Springer
- Montasari R. (ur.), H. Jahankhani (ur.), R. Hill (ur.), S. Parkinson (ur.) (2021) Digital Forensic Investigation of Internet of Things (IoT) Devices, Springer
- Wilson C. W. (2021), Cybersecurity, MIT Press
- Mitnik K. (2017) The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data, Little, Brown and Company

Cilji in kompetence:	**Objectives and competences:**
Splošne kompetence: • Razumevanje pomena kibernetske varnosti na področju interneta stvari in operativnih tehnologij • Sposobnost identifikacije kibernetskih varnostnih tveganj ter izdelave predlogov za ukrepanje in zaščito na osnovi identificiranih tveganj • Sposobnost pridobivanja, selekcije, analize informacij in zmožnost njihove interpretacije za celovito reševanje problemov, izzivov in incidentov s področja kibernetske varnosti interneta stvari in operativnih tehnologij ***Predmetno-specifične kompetence:*** • sposobnost razvoja učinkovitih sistemov za zaščito interneta stvari in operativnih tehnologij z vidika kibernetske varnosti	***General competences:*** • Understanding of the cybersecurity in the field of operational technologies and internet of things • Ability to identify cybersecurity threats and provision of protective countermeasures based on the security threats assessment • Ability to collect, select, analyze information and capability to interpret it in order to provide holistic problem resolutions, as well as challenges and incidents in the field of cybersecurity of operational technologies and internet of things ***Subject-specific competences:*** • ability to develop efficient systems of cybersecurity protection of the operational technologies and internet of things

• uporaba standardov in modelov na področju kibernetske varnosti interneta stvari in operativnih tehnologij • sposobnost priprave vdornih ter ranljivostnih testov • kompetentno spremljanje, poročanje in analiziranje podatkov na področju kibernetske varnosti interneta stvar in operativnih tehnologij • kompetentno, trajnostno zagotavljanje organizacijskih struktur za ustrezne raziskave in razvoj na področju kibernetske varnosti interneta stvari ter operativnih tehnologij	• ability to apply standards and models in the field of cybersecurity of operational technologies and internet of things • ability to prepare vulnerability and penetration tests • competent monitoring, reporting and analysing cybersecurity data from internet of things devices and operational technology • competent, sustainable provision of organizational structures for research and development in the cybersecurity field with focus on operational technologies and internet of things

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: • poznavanje zgradbe sistemov s področja interneta stvari in operativnih tehnologij • razumevanje kibernetskega sistema in pomena varnosti za delovanje interneta stvari in operativnih tehnologij • razumevanje ključne problematike varnosti na področju interneta stvari in operativnih tehnologij • poznavanje ključnih površin in vektorjev napadov, ki lahko ogrozijo delovanje kritične infrastrukture • identifikacija napadov s pomočjo programskih orodij • realizacija algoritmov za zaščito pred napadi na robni strojni opremi • razumevanje postopkov zasnove sistemov interneta stvari z minimalnimi varnostnimi tveganji • poznavanje varnostnega testiranja na področju interneta stvari in operativnih tehnologij • sposobnost detekcije vdorov na področju interneta stvari in operativnih tehnologij • razumevanje organizacijske strukture za zagotavljanje varnosti s področja interneta stvari in operativnih tehnologij • razumevanje pomena varnostnih standardov ter raziskav in razvoja na	Knowledge and understanding: • knowledge of the operational technologies and internet of things system structure • understanding of cybernetic system and importance of cybersecurity for proper functioning of operational technologies and internet of things • understanding of key security issues in the field of operational technologies and internet of things • knowledge of key surfaces of attacks and attack vectors which can compromise proper functioning of critical infrastructure • realization of algorithms for protection against attacks on the edge hardware equipment • understanding of the system design incorporating internet of things with minimal cybersecurity risk • knowledge of cybersecurity testing in the field of internet of things and operational technologies • ability to detect penetrations in the framework of operational technologies and internet of things • understanding of organizational structure for cybersecurity provision in the field of operational technologies and internet of things • understanding of the meaning of cybersecurity standards and research

področju kibernetske varnosti interneta stvari in operativnih tehnologij	and development in the field of operational technologies and internet of things

Metode poučevanja in učenja:	**Learning and teaching methods:**
• *Predavanja z aktivno udeležbo študentov* (razlaga, diskusija, vprašanja, primeri, reševanje primerov in nalog); • *Vaje*, kjer študentje na primerih ponovijo temeljne koncepte, predstavljene na predavanjih; • *Laboratorijske vaje*, kjer se študenti naučijo realizirati napredne sisteme interneta stvari in operativnih tehnologij. Na razvitih primerih se preučijo varnostna tveganja in možnosti vdorov.	• *Lectures with active participations by the students* (explanation, discussion, questions, cases, examples and problems solving); • *Tutorials*, where students will recall, basic concepts in introduced at lectures; • *Lab work*, where students will learn to realize advanced systems using operational technologies and internet of things. Security issues will be studied on developed systems and security penetration tests will be performed.

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:

- ŠKRABA, Andrej, STOJANOVIĆ, Radovan, ZUPAN, Anton, KOLOŽVARI, Andrej, KOFJAČ, Davorin. Speech-controlled cloud-based wheelchair platform for disabled persons. Microprocessors and microsystems. [Print ed.]. nov. 2015, vol. 39, no. 8, str. 819-828. ISSN 0141-9331. http://www.sciencedirect.com/science/article/pii/S0141933115001581, DOI: 10.1016/j.micpro.2015.10.004.
- ŠKRABA, Andrej, KOLOŽVARI, Andrej, KOFJAČ, Davorin, STOJANOVIĆ, Radovan, SEMENKIN, Eugene S., STANOVOV, Vladimir V. Development of cyber-physical speech-controlled wheelchair for disabled persons. V: KONOFAOS, Nikos (ur.), KITSOS, Paris (ur.). DSD 2019 : proceedings. 22nd Euromicro Conference on Digital System Design, 28-30 August 2019, Kallithea, Greece. Los Alamitos (California); Piscataway: IEEE: CPS, cop. 2019. Str. 456-463, ilustr. ISBN 978-1-7281-2861-0. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8875233, DOI: 10.1109/DSD.2019.00072.
- KOLOŽVARI, Andrej, STOJANOVIĆ, Radovan, ZUPAN, Anton, SEMENKIN, Eugene S., STANOVOV, Vladimir V., KOFJAČ, Davorin, ŠKRABA, Andrej. Speech-recognition cloud

harvesting for improving the navigation of cyber-physical wheelchairs for disabled persons. Microprocessors and microsystems. [Print ed.]. sep. 2019, vol. 69, str. 179-187. ISSN 0141-9331. https://www.sciencedirect.com/science/article/pii/S0141933119300109, DOI: 10.1016/j.micpro.2019.06.006.

- KOFJAČ, Davorin, STOJANOVIĆ, Radovan, KOLOŽVARI, Andrej, ŠKRABA, Andrej. Designing a low-cost real-time group heart rate monitoring system. Microprocessors and microsystems. [Print ed.]. nov. 2018, vol. 63, str. 75-84. ISSN 0141-9331. https://www.sciencedirect.com/science/article/pii/S0141933118301480?via%3Dihub, DOI: 10.1016/j.micpro.2018.08.010.

- ŠKRABA, Andrej, STANOVOV, Vladimir V., SEMENKIN, Eugene S., KOLOŽVARI, Andrej, KOFJAČ, Davorin. Development of algorithm for combination of cloud services for speech control of cyber-phisical systems. International Journal on Information Technologies and Security. 2018, vol. 10, no. 1, str. 73-82, tabele, graf. prikazi. ISSN 1313-8251. [COBISS.SI-ID 7997971]
- STOJANOVIĆ, Radovan, ŠKRABA, Andrej. Simplified open HW/SW pulse oximetry interface for purpose of COVID-19 symptoms detection and monitoring. V: 2021 10th Mediterranean Conference on Embedded Computing (MECO), 7-10 June 2021, Budva, Montenegro. 2021 10th Mediterranean Conference on Embedded Computing (MECO), 7-10 June 2021, Budva, Montenegro. [S. l.]: IEEE Xplore, cop. 2021. Str. 1-5, ilustr. ISBN 978-1-6654-3912-1. https://ieeexplore.ieee.org/document/9460178, DOI: 10.1109/MECO52532.2021.9460178.
- STOJANOVIĆ, Radovan, ŠKRABA, Andrej, LUTOVAC, Budimir. A headset like wearable device to track COVID-19 symptoms. V: 2020 9th Mediterranean Conference on Embedded Computing (MECO). 2020 9th Mediterranean Conference on Embedded Computing (MECO), 8-11 June 2020, Budva, Montenegro (online). [S. l.]: IEEE Xplore, cop. 2020. Str. 1-4, ilustr. https://ieeexplore.ieee.org/document/9134211.
- ŠKRABA, Andrej, KOLOŽVARI, Andrej, KOFJAČ, Davorin, STOJANOVIĆ, Radovan, SEMENKIN, Eugene S., STANOVOV, Vladimir V. Prototype of group heart rate monitoring with ESP32 : comparison to ESP8266. V: STOJANOVIĆ, Radovan (ur.), et al. Proceedings - research monograph. 2019 8th Mediterranean Conference on Embedded Computing (MECO) including ECyPS'2019, June 10-14, 2019, Budva, Montenegro. [S. l.]: Institute of Electrical and Electronics Engineers, cop. 2019. Str. 700-703, tabele. ISBN 978-1-7281-1739-3.
- ŠKRABA, Andrej, KOLOŽVARI, Andrej, KOFJAČ, Davorin, STOJANOVIĆ, Radovan. Prototype of group heart rate monitoring with NODEMCU ESP8266. V: STOJANOVIĆ, Radovan (ur.), et al. Proceedings - research monograph. 6th Mediterranean Conference on Embedded Computing (MECO) including ECyPS'2017, Bar, Montenegro, June 11th-15th, 2017. [S. l.]: Institute of Electrical and Electronics Engineers, cop. 2017. Str. 534-537, ilustr. ISBN 978-1-5090-6740-4, ISBN 978-1-5090-6741-1, ISBN 978-1-5090-6742-8.