UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Računalniška forenzika
Course title:	Computer Forensics

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-RF-2021-12-14

Predavanja Lectures	Seminar Seminar	Vaje Tutorial	Klinične vaje work	Druge oblike študija	Samost. delo Individ. work	ECTS
30	-	20	-	-	100	5

Nosilec predmeta / Lecturer:	Izr. prof. dr. Blaž Rodič

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:
Študent/študentka mora pred pristopom k izpitu pripraviti in zagovarjati seminarsko nalogo.	Prior to the exam, the student has to prepare and present seminar work.

Vsebina:	Content (Syllabus outline):
• računalniška forenzika • pregled tehnologije • digitalni dokazi • računalniški dokazi in njihovo zbiranje • forenzična analiza Windows sistemov • forenzična analiza Linux sistemov • forenzika malware-a • forenzika GSM in mobilnih naprav	• computer forensics • technology overview • digital evidence • computer evidence and their collection • forensic analysis of Windows systems • forensic analysis of Linux systems • forensics of malware-a • forensics of GSM and mobile devices • forensics of networks, internet and cloud computing

• forenzika mrež, Interneta in računalništva v oblaku • uporaba odprtokodnega orodja v računalniški forenziki • predstavitev rezultatov • zaključna razmišljanja	• the use of open source tools in computer forensics • presentation of results • concluding thoughts

Temeljni literatura in viri / Readings:

- Nelson B., Phillips A. and Steuart C.: Guide To Computer Forensics and Investigations, 6th ed., 2018, Cengage.
- Carvey H.: Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry 2nd Edition, 2016, Syngress.
- Årnes A. (Editor): Digital Forensics, 1st Edition, 2017, Wiley.

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 pridobivanja, selekcije, analize informacij in zmožnost njihove interpretacije za celovito reševanje problemov, izzivov in incidentov s področja kibernetske varnosti. • Sposobnost uporabe različnih programskih rešitev za zagotavljanje, upravljanje, nadzorovanje in evalvacijo kibernetske varnosti. ***Predmetno-specifične kompetence:*** • uporaba metodoloških orodij, tj. izvajanje, koordiniranje in organiziranje raziskav, uporaba raznih raziskovalnih metod in tehnik ter ocenitev njihove uporabnosti; • sposobnost poiskati, analizirati in ohraniti forenzične dokaze; • sposobnost samostojne izvedbe osnovne forenzične raziskave.	*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 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 use various software solutions to provide, manage, monitor and evaluate cyber security. ***Subject-specific competences:*** • use of methodological tools, i.e. implementation, coordination and organisation of research, use of various research methods and techniques and to evaluate their usefulness; • ability to search, analyse and preserve forensic evidence; • ability to independently perform basic forensic research.

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: • poiskati in ohraniti digitalne dokaze • samostojna izvedba osnovne forenzične analize živega sistema • samostojna izvedba kriminalistično-tehnične analize post-mortem sistemov • samostojna izvedba forenzične analize mobilnih in PDA naprav • izvedba analize malware-a • izvedba ocene orodij za izvajanje računalniške forenzike • predložitev in predstavitev poročila o spremljanju poslovanja	Knowledge and understanding: • locate and preserve digital evidence • independent implementation of basic forensic analysis of living systems • independent implementation of forensic analysis of post-mortem systems • independent implementation of forensic analysis of mobile and PDA devices • analyzing a malware • performance assessment tools for implementation of computer forensics • submission and presentation of a monitoring operations report

Metode poučevanja in učenja:	**Learning and teaching methods:**
• *predavanja* z aktivno udeležbo študentov (razlaga, diskusija, vprašanja, primeri, reševanje primerov) • *vaje in laboratorijske vaje* • individualne in skupinske *konzultacije* (diskusija, dodatna razlaga, obravnava specifičnih vprašanj)	• *lectures* with active participation of students (explanation, discussion, questions, examples, problem solving) • *exercises and lab work* • individual and group consultations (discussion, additional explanation, consideration of specific issues)

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt):		Type (examination, oral, coursework, project):
• pisni izpit	50 %	• written exam
• seminarska naloga s poročili seminarskega dela in eksperimentalnih vaj ter predstavitev naloge	50 %	• seminar work

Reference nosilca / Lecturer's references:

- RODIČ, Blaž. Industry 4.0 and the new simulation modelling paradigm. Organizacija : revija za management, informatiko in kadre, ISSN 1318-5454. [Tiskana izd.], aug. 2017, vol. 50, no. 3, str. 193-207, ilustr., doi: 10.1515/orga-2017-0017

- BRELIH, Marjan, RAJKOVIČ, Uroš, RUŽIČ, Tomaž, RODIČ, Blaž, KOZELJ, Daniel. Modelling decision knowledge for the evaluation of water management investment projects. Central European Journal of Operations Research, ISSN 1435-246X, 2018, vol. , iss. , str. https://link.springer.com/content/pdf/10.1007%2Fs10100-018-0600-5.pdf, doi: 10.1007/s10100-018-0600-5.
- KANDUČ, Tadej, RODIČ, Blaž. Optimisation of machine layout using a force generated graph algorithm and simulated annealing. International journal of simulation modelling, ISSN 1726-4529, 2016, vol. 15, no. 2, str. 275-287.
- RODIČ, Blaž, BAGGIA, Alenka. Dynamic airport ground crew scheduling using a heuristic scheduling algorithm. International journal of applied mathematics and informatics, ISSN 2074-1278, 2013, vol. 7, iss. 4, str. 153-163.
- RODIČ, Blaž. Mobile agents for distributed decision support systems. The International Scientific Journal of Management Information Systems, ISSN 1452-774X, 2011, vol. 6, no. 1, str. 20-27.
- RODIČ, Blaž, KLJAJIĆ, Miroljub. Accessing distributed data sources with mobile agents and XML. V: JAŠKOVÁ, Mária (ur.). ECON '05 : [selected research papers], (Research works proceedings, ISSN 0862-7908, Vol. 12, 2005). Ostrava: Technical University of Ostrava, Faculty of Economics. 2005, str. 280-287.
- RODIČ, Blaž, KLJAJIĆ, Miroljub. Integracija simulacijskih orodij v e-poslovni informacijski sistem. V: GRIČAR, Jože (ur.). Izboljšanje konkurenčnosti regije z e-poslovanjem, (Organizacija, ISSN 1318-5454, Letn. 37, 2004, št. 3). Kranj: Moderna organizacija. 2004, str. 162-167.
- ŠKRABA, Andrej, BAGGIA, Alenka, RODIČ, Blaž. Application of a group decision support system in the reform of study programmes. V: DONDON, Philippe (ur.). Recent advances in education and modern educational technologies, (Educational technologies series, 9). [S. l.: s. n.]. 2013, str. 128-134.
- RODIČ, Blaž. Issues of e-collaboration and knowledge management in media industries. V: LUGMAYR, Artur (ur.), et al. Information systems and management in media and entertainment industries, (International series on computer entertainment and media technology (Online), ISSN 2364-9488). Cham: Springer. cop. 2016.