UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Digitalna forenzika
Course title:	Digital forensics

Študijski program in stopnja Study programme and level	Modul Module	Letnik Academic year	Semester Semester
Informacijske in komunikacijske tehnologije, 2. stopnja	Napredne internetne tehnologije	1	2
Information and Communication Technologies, 2nd cycle	Advanced Internet Technologies	1	2

Vrsta predmeta / Course type	Izbirni / Elective
Univerzitetna koda predmeta / University course code:	IKT2-660

Predavanja Lectures	Seminar Seminar	Sem. vaje Tutorial	Lab. vaje Laboratory work	Druge oblike	Samost. delo Individ. work	ECTS
15	**15**			**15**	**105**	**5**

**Navedena porazdelitev ur velja, če je vpisanih vsaj 15 študentov. Drugače se obseg izvedbe kontaktnih ur sorazmerno zmanjša in prenese v samostojno delo. / This distribution of hours is valid if at least 15 students are enrolled. Otherwise the contact hours are linearly reduced and transfered to individual work.*

Nosilec predmeta / Lecturer:	Doc. dr. Tomaž Klobučar

Jeziki / Languages:	**Predavanja / Lectures:**	slovenščina, angleščina / Slovenian, English
	Vaje / Tutorial:	

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**
Zaključen študijski program prve stopnje s področja naravoslovja, tehnike ali računalništva.	Student must complete first-cycle study programmes in natural sciences, technical disciplines or computer science.

Vsebina:	**Content (Syllabus outline):**
Uvod: definicija osnovnih pojmov, tehnologija, zakonodaja, norme, trg; informacijski sistemi, varnost, kriminaliteta, protiukrepi, forenzika Računalniška kriminaliteta: narava in vrste računalniškega kriminala, motivacija kriminalnih dejanj; internetni kriminal, tehnološka umestitev in pregled, mrežni napadi in napadi na gostitelje, škodoželjno in vohunsko programje, zanikanje storitve, porazdeljeni napadi, piratstvo, zloraba zasebnosti, socialni inženiring, tehnološko vohunjenje, avtorske pravice, rasizem in	Introduction definition of basic concepts, technology, legislation, norms, market; information systems, security, computer crime, countermeasures, digital forensic Computer crime: nature and classification of computer crime, motivation for crime; computer crime, technological overview, network and host attacks, malicious software, denial of service, software piracy, intellectual property, privacy abuse, social engineering, corporate espionage, racism, xenophobia; technological

ksenofobija; tehnološki protiukrepi Zakonodajni vidiki računalniške kriminalitete: pravne in izvršilne podlage, Evropska unija, ZDA; slovenska zakonodaja, primerjave z drugimi zakonodajami; praksa pravnih in izvršilnih vidikov v Sloveniji in tujini, povezovanje mednarodnih in nacionalnih institucij; varnostne politike in njihovo izvrševanje v podjetjih ter ustanovah Digitalna forenzika: dokaz v digitalni obliki; digitalna forenzika in operacijski sistemi, pomnilniške naprave, prenosni sistemi, aplikacije in mrežni sistemi; načela digitalne forenzike; metodologije digitalne forenzike Osnovna orodja digitalne forenzike: laboratorij za digitalno forenziko; osnovna komercialna in odprtokodna orodja Praktični primeri uporabe orodij digitalne forenzike: primeri uporabe orodij, npr. X-WAYS in SleuthKit	countermeasures Computer crime and legalization: basic legalization documents and conventions, European Union, United states; Slovenian legislation compared to other legislations, legislation practice, national and international institutions cooperation, Corporate security policies Digital forensics: digital evidence, digital forensics methodologies, technology and legalization interrelations; digital forensic and operating systems, storage, mobile systems, applications and networked systems Basic digital forensics tools: digital forensic laboratory; basic commercial and open source forensic tools Practical examples of digital forensics tools: examples of tool usage, e.g. X-WAYS and SleuthKit

Temeljna literatura in viri / Readings:

Izbrana poglavja iz naslednjih knjig: / Selected chapters from the following books:

- E. Casey (Ed.), *Handbook of Digital Forensics and Investigation*. Elsevier Academic Press, 2009, ISBN: 978-0-12-374267-4
- S. Davidoff and J. Ham, *Network Forensics: tracking hackers through cyberspace*. Prentice Hall, 2012, ISBN-13: 978-0132564717
- K. J. Jones, R. Bejtlich and C. W. Rose. *Real Digital Forensics: Computer Security and Incident Response*. Addison Wesley, 2005, ISBN: 0321240693
- B. Carrier, *File System Forensic Analysis*. Addison Wesley, 2005, ISBN: 0-321-26817-2
- R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition*. Wiley Computer Publishing, 2008, ISBN 978-0470068526

Cilji in kompetence:	**Objectives and competences:**
Digitalna forenzika je znanost in umetnost zagotavljanja dokazov v digitalni obliki z zakonsko sprejemljivimi postopki in uporabo orodij digitalne forenzike, ki omogočajo preiskovalcu fizično in logično rekonstrukcijo kazensko odgovornih dejanj. V informacijski dobi je digitalna forenzika vedno pomembnejša zaradi široke uporabe informacijskih tehnologij tako v poslovnem svetu kakor tudi v zasebnem življenju. Osnovni namen predmeta je posredovati študentom teoretična in praktična znanja s področja digitalne forenzike. Predstavljene bodo različne oblike računalniškega kriminala in motivi	Digital forensics is science and art of gathering chains of digital evidence through legally compliant procedures with usage of various forensic tools that enable the investigator to reconstruct criminally liable actions at the physical and logical levels. In the information age the digital forensics has increasingly important role with widespread usage of digital technologies both in business processes and private life. The main objective of the course is to provide the students theoretical and practical knowledge in digital forensics. For this purpose the students will be introduced to various forms of computer crime

za kriminalna dejanja. Predstavljeni bodo predlagani in uveljavljeni postopki digitalne forenzike za zagotavljanje dokaza v digitalni obliki. Postopki bodo obravnavani z vidika trenutno veljavne nacionalne ter svetovne zakonodaje in prakse. V okviru predmeta bomo predstavili in praktično preskusili vrsto orodij digitalne forenzike. Pridobljeno znanje bo omogočilo študentom nadaljnje raziskave in razvoj na področju digitalne forenzike, za katere pričakujemo, da se bodo začele že v okviru individualnega dela v okviru predmeta.	and motivations of criminal activity. Current aspects of national and world wide legislation and practice will be discussed and related to digital forensics methodologies proposed and used for digital evidence provisioning. In the course a number of digital forensic tools will be presented and practically tested. Gained knowledge will enable the students to continue research and development in the field, which is expected to be carried out already through individual work in the course.

Predvideni študijski rezultati:	**Intended learning outcomes:**
Študent, ki bo uspešno končal ta predmet, bo pridobil: • Sposobnost analize, sinteze in predvidevanja rešitev ter posledic • Obvladanje raziskovalnih metod, postopkov in procesov, razvoj kritične in samokritične presoje • Sposobnost uporabe znanja v praksi • Avtonomnost v strokovnem delu • Razvoj komunikacijskih sposobnosti in spretnosti, posebej komunikacije v mednarodnem okolju • Etična refleksija in zavezanost profesionalni etiki • Kooperativnost, delo v skupini (in v mednarodnem okolju) Predmet pripravlja študente, da bodo sposobni: • razumeti in oceniti grožnje računalniškega kriminala, • poznati in razumeti možnosti preprečevanja računalniške kriminalitete, • razumeti postopke in metodologije zagotavljanje dokaza v elektronski obliki, • izbrati in uporabljati orodja digitalne forenzike	Student who completes this course successfully will acquire: • An ability to analyse, synthesise and anticipate solutions and consequences • To gain the mastery over research methods, procedures and processes, a development of the critical judgement • An ability to apply the theory in to a practice • An autonomy in the professional work • Communicational-skills development; particularly in international environment • Ethical reflection and obligation to a professional ethics • Cooperativity, team work (in international environment) This course prepares students to be able to: • Understand and evaluate computer crime threats, • Comprehend computer crime countermeasures, • Understand digital forensic procedures and methodologies for a digital evidence provisioning, • Select and use digital forensic tools

Metode poučevanja in učenja:	**Learning and teaching methods:**
Predavanja,seminar, konzultacije, individualno delo	Lectures, seminar, consultancy, individual work

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Seminarska naloga	25 %	Seminar work
Ustni zagovor seminarske naloge	25 %	Oral defense of the seminar work
Ustni ali pisni izpit	50 %	Oral or written exam

Reference nosilca / Lecturer's references:

- V. Jovanovikj, D. Gabrijelčič and **T. Klobučar**, "A conceptual model of security context," *International journal of information security*, ISSN 1615-5262, vol. 13, no. 6, pp. 571-581, 2014
- B. Ivanc and **T. Klobučar**, "Attack modeling in the critical infrastructure = Modeliranje napadov v kritični infrastrukturi," *Elektrotehniški vestnik*, ISSN 0013-5852. [Slovenska tiskana izd.], vol. 81, no. 5, pp. 285-292, 2014
- **T. Klobučar**, D. Gabrijelčič and V. Pagon, "Cross-border e-learning and academic services based on eIDs: case of Slovenia" in *eChallenges 2014 : 29-30 October, 2014 Belfast, Ireland*. Dublin: IIMC: = International Information Management Corporation, 8 pages, 2014
- P. Cigoj and **T. Klobučar**, "Cloud security and OpenStack," in R. Trobec (Ed.), *Proceedings of the 1st International Conference on CLoud Assisted ServiceS, Bled, Slovenia, October 22 -25: CLASS*. 1st ed. Ljubljana: Univerza v Ljubljani, pp. 20-27, 2012
- V. Jovanovikj, D. Gabrijelčič and **T. Klobučar**, "Access control in BitTorrent P2P networks using the enhanced closed swarms protocol" in Netware 2011: August 21-27, 2011, Nice - Saint Laurent du Var, France. [S. l.], pp. 97-102, 2011