

UČNI NAČRT PREDMETA / COURSE SYLLABUS

Predmet: FORENZIČNE PREISKAVE V INFORMATIKI
Course title: INFORMATION TECHNOLOGY FORENSIC INVESTIGATIONS

Študijski program in stopnja Study programme and level	Študijska smer Study field	Letnik Academic year	Semester Semester
Magistrski program - 2. stopnja	Forenzične preiskave v financah in računovodstvu	2	2
Master's program	Fraud Examination in Finance and Accounting	2	2

Vrsta predmeta / Course type Izbirni/elective course

Univerzitetna koda predmeta / University course code: --

Predavanja Lectures	Seminar Seminar	Vaje Tutorial	Klinične vaje work	Druge oblike študija	Samost. delo Individ. work	ECTS
40	10	10	0	0	90	6

Nosilec predmeta / Lecturer: doc.dr. Arso Savanovič/ Assistant professor Arso Savanovič PhD

Jeziki / Languages:
Predavanja / Lectures: Slovensko/slovenian
Vaje / Tutorial: Slovensko/slovenian

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

Splošno poznavanje IKT

Prerequisites:

Basic understanding of ICT

Vsebina:

- Uvod v forenzične preiskave v informatiki
- Kriptologija in informacijska varnost
- Osnove digitalne forenzike
- Preiskovalni procesi digitalne forenzike
- IKT forenzične preiskave (računalniki, podatkovni mediji, baze podatkov, mobilne naprave, omrežja, internet, e-oblak, e-pošta)
- Forenzične preiskave v e-poslovanju
- Pravni vidiki digitalne forenzike

Content (Syllabus outline):

- Introduction to the Information Technology Forensic Investigations
- Cryptography and Information Security
- Basics of Digital Forensics
- Digital Forensics Investigation Process
- ICT Forensic Investigations (Computers, Disk Media, Databases, Mobil Devices, Networks, E-Clouds, Internet, E-mails)
- Forensic Investigations in e-Business
- Legal Aspects of Digital Forensics

Temeljni literatura in viri / Readings:

Nolan R., O'Sullivan C., Branson J., Waits C. (2005), First Responders Guide to Computer Forensics, Carnegie Mellon University

Sammons J. (2012) The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, Elsevier

Casey E. (Editor) (2010), Handbook of Digital Forensics and Investigation, Elsevier

Nelson B., Phillips A., Steuart C. (2010), Guide to Computer Forensics and Investigations, 4th Edition, Course Technology

Cilji in kompetence:

Glavni cilj predmeta je seznaniti študente, da razumejo pomen in principe delovanja digitalne forenzike. Študenti pridobijo osnovna znanja o forenzičnih preiskavah v informatiki in razumejo vlogo digitalnih forenzikov v preiskovalnih procesih. Seznanijo se z osnovami kriptologije, in osnovami informacijske varnosti. Spoznajo in ločijo forenzične metode pri delu z računalniki, podatkovni mediji, bazami podatkov, mobilnimi napravami, omrežji, internetom, e-oblakom ter e-pošto. Spoznajo tudi forenzične preiskave v e-poslovanju in razumejo pravno problematiko digitalne forenzike.

Objectives and competences:

The goal of the subject is to acquire the meaning and principles of digital forensics. Students acquire the basic knowledge about forensic investigations in IT and understand the role of digital forensics in the investigation process. They learn the basics of cryptology and information security. They familiarize and distinguish forensic methods of working with computers, data media, databases, mobile devices, networks, Internet, e-cloud and e-mails. They learn about the forensic examination of e-Business and understand the legal issues of digital forensics.

Predvideni študijski rezultati:**Znanje in razumevanje:**

Poznavanje in razumevanje osnov o forenzičnih preiskavah v informatiki. Razumevanje vloge digitalnih forenzikov v preiskovalnih procesih. Poznavanje in razumevanje osnov kriptologije in informacijske varnosti. Razumevanje forenzičnih metod pri delu z računalniki, podatkovni mediji, bazami podatkov, mobilnimi napravami, omrežji, internetom, e-oblakom in e-pošto. Poznavanje forenzičnih preiskav v e-Poslovanju. Razumevanje pravne problematike digitalne forenzike.

Intended learning outcomes:**Knowledge and understanding:**

Knowing and understanding the basics of forensic investigations in informatics. Understanding the role of digital forensics in investigation processes. Knowing and understanding the basics of cryptology and information security. Understanding the forensic methods of working with computers, data media, databases, mobile devices, networks, Internet, e-cloud and e-mail. Knowledge of digital forensic investigations in e-Business. Understanding the legal issues of digital forensics.

Metode poučevanja in učenja:

Predavanja, diskusije, individualni projekti, skupinsko delo ter individualne konzultacije s predavateljem. Asistent bo s študenti izvedel vaje.

Learning and teaching methods:

Lectures, discussions, individual and group projects; individual teacher-student tutoring. Assistant conducts coursework with the students.

Načini ocenjevanja:

Delež (v %) /

Weight (in %) /

Assessment:

Seminarska naloga	40	Seminar paper
Pisni izpit	60	Written examination

Reference nosilca / Lecturer's references:**Monografije / Books**

- GABRIJELČIČ, Dušan, SAVANOVIČ, Arso. Security management. In: *Programmable networks for IP service deployment*, (Artech House telecommunications library). Boston; London:Artech House, 2004, str. 225-251

Članki v revijah in na konferencah /Journal and conference papers

- SAVANOVIČ, Arso, GABRIJELČIČ, Dušan, JERMAN-BLAŽIČ, Borka, BEŠTER, Janez. Implementation and evaluation of integrity protection facilities for active grids. *Lect. notes comput. sci.*, part 3, LNCS 3038, str. 179-186
- SAVANOVIČ, Arso, GABRIJELČIČ, Dušan, JERMAN-BLAŽIČ, Borka, KARNOUSKOS, Stamatis. An active networks security architecture. *Informatica (Ljublj.)*, 2002, vol. 26, no. 2, str. 211-221.
- GABRIJELČIČ, Dušan, SAVANOVIČ, Arso, JERMAN-BLAŽIČ, Borka. Design, implementation and evaluation of security facilities for a next generation network element. V: JERMAN-BLAŽIČ, Borka (ur.), SCHNEIDER, Wolfgang (ur.), KLOBUČAR, Tomaž (ur.). *Security and privacy in advanced networking technologies*, (NATO science series, Series 111, Computer and systems sciences, vol. 193). Amsterdam [etc.]: IOS Press, 2004, str. 115-134

Tekoči projekti / Running projects

- Survivable Ad-Hoc Networks (SAN) - mednarodni projekt na področju dinamičnih mobilnih omrežij 4. generacije, 12 partnerjev / 6 držav, program EUREKA
- KC SURE - kompetenčni center na področju rešitev in storitev za učinkovito rabo električne energije (Smart Grids), 16 partnerjev, MIZKŠ
- KC CLASS - kompetenčni center na področju storitev v računalniškem oblaku (Cloud Computing), 16 partnerjev, MIZKŠ
- Telerehabilitacija - doktorsko usposabljanje mladega raziskovalca v gospodarstvu v sodelovanju z Univerzitetnim rehabilitacijskim inštitutom (URI-SOČA), SPIRIT (bivša Tehnološka agencija RS)

Izbrani pretekli projekti / Selected past projects

- FAIN - Future Active IP Networks, FP5 - 5. Okvirni program EU, IST - Information Society Technologies (IST-1999-10561), 2000-2003
- DIADEM FIREWALL - Distributed Adaptive Security by Programmable Firewall, FP6 - 6. Okvirni program EU, IST - Information Society Technologies (IST-2002-002154), 2004-2006

Druge reference/ Other references

- Mentor doktorskega kandidata v okviru programa mladi raziskovalec v gospodarstvu
- Evalvator mednarodnih raziskovalnih projektov v EU programih FP7 in AAL

- Evalvator nacionalnih raziskovalnih projektov v sklopu ARRS