UČNI NAČRT PREDMETA / COURSE SYLLABUS (leto / year 2016/17)			
Predmet:	Informacijska varnost in zasebnost		
Course title:	Information security and privacy		

Študijski program in stopnja **Study programme and level**	**Študijska smer** **Study field**	**Letnik** **Academic year**	**Semester** **Semester**
Interdisciplinarni magistrski študijski program Računalništvo in matematika	ni smeri	1 ali 2	prvi
Interdisciplinary Master's study programme Computer Science and Mathematics	none	1 or 2	first

Vrsta predmeta / Course type	izbirni / elective
Univerzitetna koda predmeta / University course code:	63521

Predavanja **Lectures**	**Seminar** **Seminar**	**Vaje** **Tutorial**	**Klinične vaje** **work**	**Druge oblike študija**	**Samost. delo** **Individ. work**	**ECTS**
45		**30**			**105**	**6**

Nosilec predmeta / Lecturer:	prof. dr. Denis Trček

Jeziki / Languages:	**Predavanja / Lectures:**	slovenski / Slovene, angleški / English
	Vaje / Tutorial:	slovenski / Slovene, angleški / English

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**
Vpis v letnik študija.	Enrolment in the programme.
Vsebina:	**Content (Syllabus outline):**

Uvodni pregled področja.	Introduction.
Ključne organizacije in standardi (ISO, ITU-T, IETF, W3C, OASIS, OMA).	Key standards and organizations (ISO, ITU-T, IETF, W3C, OASIS, OMA).
Varnostni mehanizmi in varnostne storitve (principi in praktične izvedbe overjanja, zaupnosti, celovitosti, nezatajljivosti, nadzora dostopa, beleženja in alarmiranja) ter infrastruktura javnih ključev (časovna normala, upravljanje imenskega prostora, operativni protokoli).	Security mechanisms, security services (principles and practical implementations of authentication, confidentiality, integrity, non-repudiation, access control, logging and alarming), public key infrastructure (time base, name space management, operational protocols).
Infrastruktura za overjanje, avtorizacijo in nadzor (principi, primeri standardiziranih rešitev - RADIUS).	Authentication, authorization and accounting infrastructure (principles, examples of standardized solutions like RADIUS).
Varovanje na fizičnem in linijskem nivoju (protokoli WEP, WPA1 in WPA2).	Security of physical and data layers (example protocols are WEP, WPA1 and WPA2).
Varovanje na mrežnem, transportnem in aplikacijskem sloju s poudarkom na spletnih storitvah (protokoli IPSec, TLS, S/MIME, SET, XMLSec, SAML, XACML, WS-*).	Security of network, transport and application layers with emphasis on web services (example protocols are IPSec, TLS, S/MIME, SET, XMLSec, SAML, XACML, WS-*).
Formalne metode (taksonomija formalnih metod in primeri kot so metoda R. Rueppla, logika BAN).	Formal methods (taxonomy of formal methods, examples like R. Rueppl's method, logic BAN).
Obvladovanje zasebnosti (senzorske mreže, rešitve RFID) in obvladovanje zaupanja ter ugleda v storitvenih arhitekturah.	Privacy management and privacy by design (sensor networks, RFID systems) with trust management and reputation management basics in services oriented architectures.
Osnove varnostnega programskega inženirstva.	Fundamentals of security engineering.
Obvladovanje tveganj pri varovanju informacijskih sistemov, organizacijski pristopi ter obvladovanje človeškega dejavnika (varnostne politike, modeliranje človeškega dejavnika in simulacije).	Risk management in IS, organizational views and human factor views (security policies, human factor modeling and simulations).
Akreditacijski in nadzorno-revizijski postopki varnosti informacijskih sistemov (ISO 2700X, CISSP) ter evalvacijski postopki za zagotavljanje	Accreditation and auditing of IS related to security (ISO 2700X, CISSP), and standards for technical implementations of hardware and software components (Common Criteria).
	Basic legislation in the area of IS security and

varnosti strojno-programskih komponent (Common Criteria). Temeljna zakonodaja (direktive EU in nacionalne implementacije).	privacy (EU directives, national implementations).

Temeljni literatura in viri / Readings:

D. Trček: Information Systems Security and Privacy, Springer, New York, Heidelberg, 2006.

D. Trček, Informacijska varnost in zasebnost, kopije prosojnic, FRI UL 2009.

Cilji in kompetence:	**Objectives and competences:**
Cilj predmeta je, da študentje aktivno osvojijo znanja varovanja omrežij in zasebnosti v sodobnih informacijskih sistemih in sicer za namen skrbništva (administracije), kot tudi namen razvoja novih rešitev.	The goal of the course is to educate students to be able to actively provide security and privacy in contemporary information systems, be it as systems administrators, or developers of new solutions.

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: Poznavanje principov varovanja računskih virov in podatkov (zasebnosti) v sodobnih globalnih informacijskih okoljih. Uporaba: Aplikacija na nivoju skrbništva informacijskih sistemov in na nivoju razvoja ter raziskav področja varnosti in zasebnosti. Refleksija: Holistično razumevanje obvladovanja informacijske varnosti in zasebnosti. Prenosljive spretnosti - niso vezane le na en	Knowledge and understanding: Knowledge of the principles for protection of computing resources, data, and privacy in a modern global information environment. Application: Administration of security and privacy IS solutions, and their development. Reflection: Holistic understanding of information security and privacy. Transferable skills: The course is related to areas of operating systems, computer communications, and business views of IS

predmet: Predmet se navezuje na problematiko op. sistemov, računalniških komunikacij in poslovnega vidika obvladovanja informacijskih sistemov.	security and privacy.

Metode poučevanja in učenja:	**Learning and teaching methods:**
Predavanja, demonstracije na predavanjih, praktično delo na vajah, izdelava seminarskih nalog.	Lectures, demonstrations during lectures, practical laboratory work, seminal works.

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt): Sprotno preverjanje (domače naloge, kolokviji in projektno delo) Končno preverjanje (pisni in ustni izpit) Ocene: 6-10 pozitivno, 1-5 negativno (v skladu s Statutom UL)	 50% 50%	Type (examination, oral, coursework, project):Continuing (homework, midterm exams, project work)Final (written and oral exam) Grading: 6-10 pass, 1-5 fail (according to the rules of University of Ljubljana)

Reference nosilca / Lecturer's references:

TRČEK, Denis. Managing information systems security and privacy. Berlin, Heidelberg, New York: Springer, 2006. XIII, 235 str., ilustr. ISBN 3-540-28103-7. ISBN 978-3-540-28103-0. [COBISS.SI-ID 19469863]

TRČEK, Denis. A formal apparatus for modeling trust in computing environments. Mathematical and computer modelling, ISSN 0895-7177. [Print ed.], Jan. 2009, vol. 49, no. 1/2, str. 226-233, ilustr. [COBISS.SI-ID 6557012]

TRČEK, Denis, KOVAČ, Damjan. Formal apparatus for measurement of lightweight protocols. Computer standards & interfaces, ISSN 0920-5489. [Print ed.], Feb. 2009, vol. 31, no. 2, str. 305-308, ilustr. [COBISS.SI-ID 2557399]

TRČEK, Denis. Security metrics foundations for computer security. The Computer journal, ISSN 0010-4620, 2010, vol. 53, no. 5, str. 1106-1112. [COBISS.SI-ID 1024172628]

TRČEK, Denis, ABIE, Habtamu, SKOMEDAL, Åsmund, STARC, Iztok. Advanced framework for digital forensic technologies and procedures. Journal of forensic sciences, ISSN 0022-1198, Nov. 2010, vol. 55, no. 6, str. 1471-1480, ilustr. [COBISS.SI-ID 7844692]