UČNI NAČRT PREDMETA / COURSE SYLLABUS	
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 in 2	prvi
Interdisciplinary Masters study programme Computer Science and Mathematics	none	1 in 2	first

Vrsta predmeta / Course type	izbirni
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:	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:**
Vsebina:	**Content (Syllabus outline):**

Uvodni pregled področja. Ključne organizacije in standardi (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), infrastruktura javnih ključev (časovna normala, upravljanje imenskega prostora, operativni protokoli), osnove kvantnega procesiranja (kvantna izmenjava ključev). Infrastruktura za overjanje, avtorizacijo in nadzor (principi, primeri standardiziranih rešitev – RADIUS in Diameter). Varovanje na fizičnem in linijskem sloju (protokoli WEP, WPA1 in WPA2). Varovanje na mrežnem, transportnem in aplikacijskem sloju, vključno z internetom stvari in računalništvom v oblaku (protokoli IPSec, TLS, S/MIME, SET, XMLSec, SAML, XACML, WS-*). Formalne metode (taksonomija formalnih metod in primeri kot so metoda R. Rueppla, logika BAN). Obvladovanje zasebnosti (senzorske mreže, rešitve RFID) in obvladovanje zaupanja ter ugleda v storitvenih arhitekturah. Varnostno usmerjeno programsko inženirstva (prverjanje modelov). Obvladovanje tveganj pri varovanju informacijskih sistemov, organizacijski pristopi ter obvladovanje človeškega dejavnika (varnostne politike, modeliranje človeškega dejavnika in simulacije). Akreditacijski in nadzorno-revizijski postopki varnosti informacijskih sistemov (ISO 2700X,		Introduction. Key standards and organizations (ISO, ITU-T, IETF, W3C, OASIS, OMA). 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), quantum computing basics (quantum key exchange). Authentication, authorization and accounting infrastructure (principles, examples of standardized solutions like RADIUS and Diameter). Security of physical and data layers (example protocols are WEP, WPA1 and WPA2). Security of network, transport and application layers, including internet of things and clouds (example protocols are IPSec, TLS, S/MIME, SET, XMLSec, SAML, XACML, WS-*). Formal methods (taxonomy of formal methods, examples like R. Rueppl's method, logic BAN). Privacy management and privacy by design (sensor networks, RFID systems) with trust management and reputation management basics in services oriented architectures. Secure programming (model checking). Risk management in IS, organizational views and human factor views (security policies, human factor modelling and simulations). 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

CISSP) ter evalvacijski postopki za zagotavljanje varnosti strojno-programskih komponent (Common Criteria). Temeljna zakonodaja (direktive EU in nacionalne implementacije). Zaključki. Addendum: Mini vložki s praktičnim delom, ki pokrivajo najnovejše trende.	privacy (EU directives, national implementations). Comclusions. Addendum: Mini practical tasks covering the latest selected technological issues.

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 2017/2018.

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. Kategorizirane kompetence: -Razvijanje sposobnosti kritičnega, analitičnega in sintetičnega razmišljanja. -Sposobnost definiranja, razumevanja in reševanja kreativnih profesionalnih izzivov na področju računalništva in informatike. -Sposobnost profesionalnega komuniciranja v materinem in tujem jeziku. -Sposobnost biti skladen z varnostnimi, funkcionalnimi in okoljskimi zahtevami. -Sposobnost razumevanja in uporabe znanja računalništva in informatike na drugih	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. Categorized competences: - Developing skills in critical, analytical and synthetic thinking. - The ability to define, understand and solve creative professional challenges in computer and information science. - The ability of professional communication in the native language as well as a foreign language. - Compliance with security, functional, economic and environmental principles. - The ability to understand and apply computer

relevantnih področjih (ekonomija, organizacija, umetnost, itd.). -Praktična znanja in sposobnosti na področju strojne in programske opreme ter informacijske tehnologije za uspešno profesionalno delo.	and information science knowledge to other technical and relevant fields (economics, organisational science, fine arts, etc). -Practical knowledge and skills of computer hardware, software and information technology necessary for successful professional work in computer and information science.

Predvideni študijski rezultati:	**Intended learning outcomes:**
Po zaključku predmeta bo študent: -poznal in razumel principe varovanja informacijskih sistemov ter zagotavljanja zasebnosti, -poznal in razumel standardne rešitve na tem področju, -sposoben operativno upravljati informacijske sisteme s stališča zagotavljanja varnosti in zasebnosti, -znal razvijati enostavnejše varnostne rešitve, -sposoben interne revizije informacijskih sistemov s stališča varnosti, -znal specificirati varnostno politiko.	After completing this course a student will: -know and be familiar with principles for providing security and privacy in information systems, -know and understand standard solutions in this area, -be able to administer security and privacy of information systems, -be able to develop simpler solutions in this domain, -be qualified for internal security and privacy auditing, -be able to define security policy.

Metode poučevanja in učenja:	**Learning and teaching methods:**
Predavanja, vaje s projektnim delom (praktične prototipne implementacije), lastne predstavitve. Udeležba na vajah je obvezna (zahtevan procent udeležbe se določi ob začetku študijskega leta). Nosilec predmeta lahko določi obvezno	Lectures, laboratory work (with practical prototype implementations), students' presentations. Attendance of laboratory work is mandatory (the exact percentage is announced at the beginning of a study year). The lecturer may impose mandatory attendance

udeležbo tudi na predavanjih.	of lectures.

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
50 % ocene predstavlja sprotno delo študenta v obliki preverjanj na vajah (domače naloge, kvizi, praktičen projekt), 50 % ocene pa predstavlja izpit, ki je načeloma v pisni obliki, lahko pa tudi v pisni in ustni obliki (pri čemer lahko nosilec namesto ustnega izpita uvede zagovor seminarja). Za uspešno opravljene obveznosti pri predmetu morata biti pozitivni obe delni oceni. Pristop k pisnemu izpitu je možen le po uspešno opravljenih obveznostih pri vajah (in v primeru dodatnih zahtev, ki se nanašajo na predavanja, po izpolnitvi le-teh). Ocene: 6-10 pozitivno, 5 negativno (v skladu s Statutom UL).	50% 50%	50% of the final grade is obtained on the basis of on-going laboratory work (home-works, quizzes, practical project implementations and presentations). The other 50% is obtained on the basis of a written exam, or written and oral exam (the lecturer may decide that a coursework replaces the oral exam). To be eligible for the written exam, a candidate must have successfully completed laboratory work, and fulfilled other obligations related to lecturing that the lecturer may have imposed. For successful completition of the course both grades have to be positive. Grading: 6-10 pass, 5 fail (according to the rules of University of Ljubljana).

Reference nosilca / Lecturer's references:

Denis Trček:

– 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. 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, 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]

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