UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Varnost v internetnih tehnologijah
Course title:	Security in Internet Technologies

Študijski program in stopnja Study programme and level	Modul Module	Letnik Academic year	Semester Semester
Informacijske in komunikacijske tehnologije, 3. stopnja	Napredne internetne tehnologije	1	1
Information and Communication Technologies, 3rd cycle	Advanced Internet Technologies	1	1

Vrsta predmeta / Course type Izbirni / Elective

Univerzitetna koda predmeta / University course code: IKT3-668

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 študij druge stopnje s področja informacijskih ali komunikacijskih tehnologij ali zaključen študij druge stopnje na drugih področjih z znanjem osnov s področja predmeta. Potrebna so tudi osnovna znanja matematike, računalništva in informatike.	Completed second cycle studies in information or communication technologies or completed second cycle studies in other fields with knowledge of fundamentals in the field of this course. Basic knowledge of mathematics, computer science and informatics is also requested.

Vsebina:	**Content (Syllabus outline):**
Uvod: predstavitev osnovnih pojmov, grožnje, napadi, varnostne storitve in mehanizmi Varnostni modeli: formalni varnostni modeli, principi načrtovanja varnih internetnih tehnologij Napredni kriptografski mehanizmi: simetrična in asimetrična kriptografija, izmenjava ključev, enosmerne zgoščevalne funkcije, digitalni podpis, časovni žig,	Introduction: presentation of basic concepts, threats, attacks, security services and mechanisms Security models: formal security models, security design principles Advanced cryptographic mechanisms: symmetric and asymmetric cryptography, key management, one-way hash functions, digital signature, timestamp, authentication mechanisms

mehanizmi overjanja Avtorizacija in nadzor dostopa: upravljanje in izvedba nadzora dostopa, požarni zid, sistemi za odkrivanje vdorov, SAML, XACML Omrežni varnostni protokoli: varnostne storitve in mehanizmi v različnih omrežnih slojih (npr. IPsec), zaščita v različnih tipih omrežij, varnost brezžičnih omrežij (IEEE 802.11, IEEE 802.16) Varnostne infrastrukture: infrastruktura javnih ključev, infrastruktura za upravljanje s privilegiji, infrastruktura za uporabo čezmejnih storitev Izbrana poglavja iz varnosti naprednih internetnih tehnologij (npr. varnost pri računalništvu v oblaku)	Authorisation and access control: management and implementation of access control, firewall, intrusion detection system, SAML, XACML Network security protocols: security services and mechanisms at different network layers (e.g. IPsec), protection in different types of networks, wireless networks security (IEEE 802.11, IEEE 802.16) Security infrastructures: public-key infrastructure, privilege management infrastructure, infrastructure for cross-border services Selected topics in advanced internet technologies security (e.g. security in cloud computing)

Temeljna literatura in viri / Readings:

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

- W. Stallings and L. Brown, *Computer Security – Principles and Practice*. Pearson 4th Edition, 2017, ISBN 978-0134794105
- R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Second Edition. Wiley Computer Publishing, 2008, ISBN 978-0470068526
- M. Bishop, *Computer security: art and science*. Addison-Wesley, 2003, ISBN 978-0201440997

Izbrani znanstveni članki iz revij s področja varnosti internetnih tehnologij, npr. Computers & Security, Network Security, Journal of Computer Security, International Journal of Information Security / Selected scientific articles in the area of information technologies security, e.g. Computers & Security, Network Security, Journal of Computer Security, International Journal of Information Security.

Cilji in kompetence:	**Objectives and competences:**
Namen predmeta je študentom predstaviti varnostne probleme v internetu in osnovne varnostne storitve in mehanizme za izboljšavo ravni varnosti v internetnih tehnologijah. Študenti bi morali biti sposobni: • Analizirati stanje varnosti in oceniti varnostne grožnje • Izbrati ustrezne metode za zagotovitev varnosti internetnih tehnologij • Načrtovati zaščito informacijskega sistema in njegovih virov • Zadostiti varnostnim zahtevam pri razvoju informacijskih aplikacij in rešitev • Razvijati varnostne ukrepe • Nadaljevati raziskovalno-razvojno delo na področju informacijske varnosti	The main objective of this course is to present security problems in Internet and basic security services and mechanisms that can be used to increase security level in internet technologies. Students should be able to: • Analyze an information system with respect to security and evaluate security threats • Select appropriate methods for internet technology security provision • Design how to protect an information system and its resources • Ensure that security requirements are met when developing information applications and solutions • Develop security measures • Continue research and development work in the area of information system security

Predvideni študijski rezultati:	**Intended learning outcomes:**
Študenti bodo z uspešno opravljenimi obveznostmi tega predmeta pridobili: • Poznavanje varnostnih problemov v internetu in ustreznih tehnoloških zaščitnih ukrepov • Sposobnost analize stanja varnosti in ocene varnostne grožnje • Sposobnost izbire ustreznega varnostnega mehanizma v danem kontekstu • Sposobnost evalvacije ustreznosti varnostnih mehanizmov • Sposobnost priprave znanstvenih rezultatov na področju	Students successfully completing this course will acquire: • Knowledge on internet security problems and relevant internet protection technologies • Ability to analyse state of security and evaluate security threats • Ability to select an appropriate security mechanism in particular context • Ability to evaluate security mechanisms • Ability to provide research results in the field

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	25 %	Oral defense
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