UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Varnost informacijskih sistemov
Course title:	Information Systems Security

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: IKT2-661

Predavanja Lectures	Seminar Seminar	Sem. vaje Tutorial	Lab. vaje Laboratory work	Druge oblike	Samost. delo Individ. work	ECTS
30	**30**			**30**	**210**	**10**

**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: predstavitev osnovnih pojmov, informacijski sistem, grožnje, napadi, osnovne varnostne storitve in mehanizmi Grožnje in napadi: vrste groženj in napadov na informacijski sistem (npr. prisluškovanje, pretvarjanje, prevzem seje, onemogočanje storitve, socialni inženiring), ranljivosti informacijskega sistema, zlonamerni programi (virus, črv, Trojanski konj, zadnja vrata) Varnostne politike: elementi varnostne politike, fizični, administrativni in tehnični zaščitni ukrepi,	Introduction: presentation of basic concepts, information system, threats, attacks, basic security services and mechanisms Threats and attacks: types of threats and attacks (e.g. sniffing, masquerading, session hijacking, denial of service, social engineering), information system vulnerabilities, malware (virus, worm, Trojan horse, back door) Security policies: security models, security policy elements, physical, administrative and technical protection methods, risk management, security economics

upravljanje s tveganji, ekonomika zaščite (stroškovno optimalna izbira varnostnih ukrepov), standard ISO/IEC 27000

Osnove kriptografije:

simetrična kriptografija (tokovne šifre, bločne šifre, kriptoalgoritmi, npr. AES, IDEA, RC2, DES), asimetrična kriptografija (Diffie-Hellman, RSA, algoritmi na podlagi eliptičnih krivulj), izmenjava ključev, enosmerne zgoščevalne funkcije, digitalni podpis, časovni žig, orodja za šifriranje in digitalno podpisovanje

Infrastruktura javnih ključev:

digitalno potrdilo, overitelj, elementi infrastrukture javnih ključev

Overjanje:

gesla, enkratna gesla, kriptografske metode za overjanje, biometrične metode, sistemi za enkratno prijavo

Avtorizacija in nadzor dostopa:

upravljanje in izvedba nadzora dostopa do informacijskega sistema, infrastruktura za upravljanje s privilegiji, AAA (Radius, Diameter), požarni zid (paketni filter, tokokrožni prehod, aplikativni zastopnik itd.), sistemi za odkrivanje vdorov

Omrežna varnost:

varnostne storitve in mehanizmi v različnih omrežnih slojih, zaščita v različnih tipih omrežij, varnost brezžičnih omrežij

Varnost aplikacij:

elektronska pošta, svetovni splet, varnost in XML, podatkovne baze

(cost optimal selection of security measures), ISO/IEC 27000

Basic cryptography:

Symmetric cryptography (stream ciphers, block ciphers, cryptoalgorithms, e.g. AES, IDEA, RC2, DES), asymmetric cryptography (Diffie-Hellman, RSA, elliptic curve cryptosystems), key management, one-way hash functions, digital signature, timestamp, encryption and signature tools

Public-key infrastructure:

public-key certificate, certification authority, public-key infrastructure elements

Authentication:

passwords, onetime passwords, cryptographic authentication mechanisms, biometric methods, single sign-on

Authorisation and access control:

management and implementation of information system access control, privilege management infrastructure, AAA (Radius, Diameter), firewall (packet filtering, circuit gateway, application proxy, etc.), intrusion detection system

Network security:

security services and mechanisms at different network layers, protection in different types of networks, wireless networks security (IEEE 802.11, IEEE 802.16)

Application security:

secure e-mail, secure world wide web, XML security, databases

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 International Edition, 2008, ISBN 978-0-13-513711-6
- 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
- R. Bojanc, B. Jerman-Blažič and M. Tekavčič, *Informacijska varnost v podjetniškem okolju: potrebe, ukrepi in ekonomika vlaganj*, (Znanstvene monografije Ekonomske fakultete). Ljubljana: Ekonomska fakulteta, 2014. VI, 168 pages, ilustr. ISBN 978-961-240-283-9

Cilji in kompetence:

Zagotovljena varnost je eden od ključnih pogojev za izvedbo večine informacijskih storitev. Cilj tega predmeta je celovito in z različnih vidikov predstaviti področje varovanja informacijskih

Objectives and competences:

Security is one of the most crucial requirements for implementing information services. The goal of this course is to provide from different points of view a broad overview of the technology, services and

sistemov. Študentje pridobijo tako teoretično kot tudi praktično znanje s področja varnostnih ukrepov, na primer o varnostnih postopkih, kriptografskih algoritmih, omrežnih varnostnih protokolih, infrastrukturi javnih ključev ali sistemih za nadzor dostopa. Predstavljene so najnovejše varnostne tehnologije, kot so biometrija, tehnologije za zaščito brezžičnih omrežij in sistemi za odkrivanje vdorov v informacijski sistem. Pridobljeno znanje in izkušnje študentom omogočajo uporabo in razvoj varnostnih tehnologij s ciljem zaščite virov informacijskega sistema. Cilj predmeta je usposobiti študente, da znajo analizirati stanje varnosti informacijskega sistema, oceniti varnostne grožnje, izbrati najustreznejše metode za zagotovitev varnosti in dejansko zaščititi vire informacijskega sistema oziroma omrežja. Študentje bodo pri razvoju lastnih informacijskih aplikacij in rešitev zmožni zadostiti varnostnim zahtevam, ki jih postavljajo okolje, zakonodaja in standardi. Pridobljeno znanje jim omogoča nadaljevanje raziskovalno-razvojnega dela na področju informacijske varnosti.	applications for information systems protection. The students will gain theoretical and practical knowledge in information security measures, such as cryptographic algorithms, network security protocols, public key infrastructures or access control methods. The most recent security technologies and applications, such as biometrics, secured wireless network or intrusion detection systems will also be presented. Gained knowledge will enable the students to use and develop security technologies. The students will be able to analyze an information system with respect to security, evaluate security threats, select appropriate protection measures and implement them. When developing their own information applications and solutions the knowledge will enable the students to meet the security requirements imposed by environment, legislation and standards. The students will also be able to continue research and development work in the area of information system security.

Predvideni študijski rezultati:	**Intended learning outcomes:**
Študent, ki bo uspešno končal ta predmet, bo pridobil: • Znanje in razumevanje o zaščiti informacijskih sistemov • 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: • Analizirati stanje varnosti informacijskega	Student who completes this course successfully will acquire: • Knowledge and understanding of how to protect information systems • 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: • Analyze an information system with respect to

sistema in oceniti varnostne grožnje • Izbrati ustrezne metode za zagotovitev varnosti informacijskega sistema • Zaščititi informacijski sistem in njegove vire • Zadostiti varnostnim zahtevam pri razvoju informacijskih aplikacij in rešitev • Razvijati varnostne ukrepe • Nadaljevati raziskovalno-razvojno delo na področju informacijske varnosti	security and evaluate security threats • Select appropriate methods for information system security provision • 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

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 1th 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 uisng the enhanced closed swarms protocol" in Netware 2011: August 21-27, 2011, Nice - Saint Laurent du Var, France. [S. l.], pp. 97-102, 201