|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **UČNI NAČRT PREDMETA / COURSE SYLLABUS** | | | | | | | | | | | | | | | | | |
| **Predmet:** | | | Varnost informacijsko komunikacijskih sistemov | | | | | | | | | | | | | | |
| **Course title:** | | | Information and communication systems security | | | | | | | | | | | | | | |
|  | | | | |  | | | | | | | |  | |  | | |
| **Študijski program in stopnja**  **Study programme and level** | | | | | **Študijska smer**  **Study field** | | | | | | | | **Letnik**  **Academic year** | | **Semester**  **Semester** | | |
| Podiplomski magistrski študijski program druge stopnje Elektrotehnika | | | | | Informacijsko komunikacijske tehnologije | | | | | | | | 2 | | 1 | | |
| 2nd cycle masters study programme in Electrical Engineering | | | | | Information and communication technologies | | | | | | | | 2 | | 1 | | |
|  | | | | | | | | | | | | | | | | | |
| **Vrsta predmeta / Course type** | | | | | | | | | | | | Obvezni-strokovni / compulsory professional | | | | | |
|  | | | | | | | | | | | |  | | | | | |
| **Univerzitetna koda predmeta / University course code:** | | | | | | | | | | | | 64299 | | | | | |
|  | | | | | | | | | | | | | | | | | |
| **Predavanja**  **Lectures** | **Seminar**  **Seminar** | | | **Vaje**  **Tutorial** | | | **Klinične vaje**  **work** | | | | **Druge oblike študija** | | | **Samost. delo**  **Individ. work** | |  | **ECTS** |
| 45 |  | | | 30 | | |  | | | |  | | | 75 | |  | 6 |
|  | | | | | | | | | | | | | | | | | |
| **Nosilec predmeta / Lecturer:** | | | | | Sašo Tomažič | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | |
| **Jeziki /**  **Languages:** | | **Predavanja / Lectures:** | | | | slovenski / Slovenian | | | | | | | | | | | |
| **Vaje / Tutorial:** | | | | slovenski / Slovenian | | | | | | | | | | | |
| **Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:** | | | | | | | | |  | **Prerequisits:** | | | | | | | |
| Vpis v letnik predmeta | | | | | | | | |  | Enrolment in the year of the course | | | | | | | |
| **Vsebina:** | | | | | | | |  | | **Content (Syllabus outline):** | | | | | | | |
| Vidiki varnosti (avtentičnost, zasebnost, tajnost, nezanikanje, dostopnost). Varovanje komunikacijsko informacijskih sistemov (varnostna politika, nevarnosti, avtentikacija, avtorizacija, požarni zidovi, protivirusna zaščita). Pretočni šifrirni postopki. Simetrični bločni šifrirni postopki (DES, IDEA, AES). Asimetrični šifrirni postopki (eksponentna izmenjava ključev, RSA, eliptične krivulje). Zgostitvene funkcije (MD5, SH1). Digitalni podpis. Upravljanje s ključi (overila, overjanje, infrastruktura javnih ključev). Kriptoanaliza. | | | | | | | |  | | Aspects of security (authentication, privacy, confidentiality, non-repudiation, accessibility). Protection of communication and information systems (security policy, threats, authentication, authorization, firewalls, anti-virus protection). Stream chippers. Symmetric key encryption (DES, IDEA, AES). Asymmetric key encryption (exponential key exchange, RSA, elliptic curves). Hash functions (MD5, SH1). Digital signature. Key management (certificates, authentication, public key infrastructure). Cryptanalysis. | | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Temeljni literatura in viri / Readings:** | | | | | |
| 1. Sašo Tomažič, Varnost informacijsko komunikacijskih sistemov, 2014 (Objavljena elektronska knjiga kot študijsko gradivo). 2. A. J. Menezes, P. C. Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997. 3. G. J. Simmons (editor), Contemporary Criptology, The Science of Information Integrity, IEEE Press, 1991. 4. M. Jagodič, S. Tomažič (urednika), Varnost in zaščita v telekomunikacijskih omrežjih. Elektrotehniška zveza Slovenije, Ljubljana, 1997. | | | | | |
| **Cilji in kompetence:** | |  | | **Objectives and competences:** | |
| Spoznavanje osnovnih principov varovanja podatkov tako pri prenosu kot shranjevanju in dostopu do podatkov. Spoznavanje nevarnosti in različnih načinov za zagotavljanje varnosti informacijsko komunikacijskih sistemov. | |  | | Understanding the basic principles of data protection during their transfer and storage. Understanding security in data access. Understanding the threats and different ways to secure information and communication systems. | |
| **Predvideni študijski rezultati:** | | |  | **Intended learning outcomes:** | |
| Študentje bodo spoznali nevarnosti, ki pretijo informacijskim sistemom in spoznali osnovne načine, kako se zaščititi pred temi nevarnostmi. | | |  | Students will understand the threats to information systems and learn the basic ways to protect against these threats. | |
|  | | |  |  | |
| **Metode poučevanja in učenja:** | | |  | **Learning and teaching methods:** | |
| Predavanja na katerih se študent seznani s teoretičnimi osnovami, in laboratorijske vaje, kjer nekaj problemov spozna tudi praktično in jih skuša v duhu timskega dela reševati. | | |  | Lectures and lab work. In lectures the students gain theoretical background and in lab they gain some practical experience. | |
| **Načini ocenjevanja:** | Delež (v %) /  Weight (in %) | | | | **Assessment:** |
| Ocene od 1 do vključno 5 so negativne, ocene od vključno 6 do 10 so pozitivne.  Pozitivna ocena vaj je pogoj za pristop k izpitu.  Prispevki k oceni:  Laboratorijske vaje  Pisni izpit | 30%  70% | | | | Negative grades: from 1 to 5, positive grades: from 6 to 10.  Positive exercises is a prerequisite for the exam.  Contributions to final grade:  Laboratory exercises  Written exam. |
| **Reference nosilca / Lecturer's references:** | | | | | |
| 1. TOMAŽIČ, Sašo (urednik, avtor). VIKING : varna informacijsko komunikacijska infrastruktura naslednje generacije : zaključno poročilo o rezultatih opravljenega raziskovalnega dela na projektu v okviru ciljnega raziskovalnega programa (CRP) "Znanje za varnost in mir 2004-2010". Ljubljana: Univerza, Fakulteta za elektrotehniko, 2006. 2. TOMAŽIČ, Sašo, VIDMAR, Tone, CIGLARIČ, Mojca, PANČUR, Matjaž, KREVL, Andrej, ZAVEC, Aleš, KOS, Anton. Varnostne politike in standardi varovanja informacij : projekt "Viking". Ljubljana: Univerza v Ljubljani, 2005. 3. TOMAŽIČ, Sašo. Varnost v telekomunikacijah in kako jo zagotoviti. Štirinajsta delavnica o telekomunikacijah, Brdo pri Kranju, 2003, str. 9-14. 4. ŽNIDAR, Simon, TOMAŽIČ, Sašo. Načrtovanje varnostne politike. Peta delavnica o telekomunikacijah, Brdo pri Kranju, 1997, str.1-10. 5. TOMAŽIČ, Sašo. Celovitost podatkov in veda o šifriranju, Peta delavnica o telekomunikacijah, Brdo pri Kranju, 1997. str. 1-14. | | | | | |