| | UČNI NAČRT PREDMETA/COURSE SYLLABUS |
|---|---|
| **Predmet** | **Varnost računalniških sistemov** |
| **Course title** | **Security of Computer Systems** |

| Študijski program in stopnja<br>Study programme and level | Študijska smer<br>Study field | Letnik<br>Academic year | Semester<br>Semester |
|---|---|---|---|
| Poslovna informatika / 1. stopnja | Računalništvo in informatika | 2. letnik | 4. |
| Business Informatics / 1st Cycle | Computer and Information Science | 2nd year | 4th |

| | |
|---|---|
| **Vrsta predmeta/Course type** | obvezni/obligatory |
| **Univerzitetna koda predmeta/University course code** | 1_RI_2_UN7 |

| Predavanja<br>Lectures | Seminar<br>Seminar | Sem. vaje<br>Tutorial | Lab. vaje<br>Laboratory work | Teren. vaje<br>Field work | Samost. delo<br>Individ. work | ECTS |
|---|---|---|---|---|---|---|
| 30 | | | 30 | | 90 | 6 |

| | |
|---|---|
| **Nosilec predmeta/Lecturer:** | doc. dr. Alenka Rožanec |

| | | |
|---|---|---|
| **Jeziki/ Languages:** | **Predavanja/Lectures:** | slovenski/Slovenian |
| | **Vaje/Tutorial:** | slovenski/Slovenian |

| **Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:** | **Prerequisites:** |
|---|---|
| • Vpis v drugi letnik študijskega programa.<br>• Študent mora pred izpitom pripraviti in predstaviti seminarsko nalogo. | • The prerequisite for inclusion is enrolment in the second year of study.<br>• Students have to successfully prepare and present a seminar paper before the examination. |

| **Vsebina:** | **Content (Syllabus outline):** |
|---|---|
| • *Temeljni pojmi s področja informacijske varnosti:* zaupnost, razpoložljivost in celovitost informacijskih virov in v njih vsebovanih informacij, grožnje, ranljivosti, varnostna tveganja, varnostni incidenti.<br>• *Pregled groženj in ranljivosti informacijskih virov:* neavtoriziran dostop, sistemske napake, uporabniške napake, naravne nesreče, zlonamerna programska | • *Basic concepts in the field of information security:* confidentiality, availability, integrity of information resources and information, threads, vulnerabilities, security risks, security incidents.<br>• *Overview of threats and vulnerabilities of information resources:* unauthorized access, system errors, user errors, natural disasters, malicious software, |

| | |
|---|---|
| oprema, različne vrste napadov (denial of service, man-in-the-middle, fishing, spoofing, socialni inženiring, SQL injection…), ranljivosti programske opreme, nepravilnost varnostnih postopkov, neznanje uporabnikov. | various types of attacks (and denial of service, man-in-the-middle, fishing, spoofing, social engineering, SQL injection ...), software vulnerabilities, irregularity of security procedures, low knowledge and awareness of users. |
| • *Postopki za zagotavljanje informacijske varnosti:* ozaveščanje o varnosti, nadzor dostopa, skrbništvo računov, upravljanje varnostnih incidentov, upravljanje pomanjkljivosti in nameščanje popravkov, upravljanje tveganj, upravljanje oddaljenega dostopa, sprejemljiva raba različnih informacijskih virov, varnostni pregledi, etični heking. | • *Procedures for providing information security:* security awareness, access control, accounting, incident management, vulnerability/patch management, risk management, remote access management, acceptable use of various information resources, security checks, ethical hacking. |
| • *Pregled ključnih varnostnih tehnologij in njihova uporaba za zmanjšanje varnostih tveganj*: avtentikacijski in avtorizacijski mehanizmi, protivirusni programi, mehanizmi za nadzor dostopa, filtriranje URL/WEB vsebine, požarni zid, VPN-povezave, sistemi za preprečevanje in zaznavanje vdorov (IDS), orodja za skeniranje in analiziranje, orodja za upravljanje mobilnih naprav (MDM). | • *Overview of key security technologies and their application to mitigate security incidents:* authentication and authorization mechanisms, antivirus software, access control mechanisms, URL/WEB filtering, firewall, VPN-connections, intrusion detection and prevention systems, scanning and analysis tools, mobile device management tools (MDM). |
| • *Kriptografija:* zgodovina in namen kriptografije, proces enkripcije in dekripcije, vrste kriptografskih algoritmov (simetrični, asimetrični) in njihova uporaba za zagotavljanje varnosti informacijskih sredstev, infrastruktura javnih ključev (PKI), elektronski podpis. | • *Cryptography:* history and purpose of cryptography, encryption and decryption process, the types of cryptographic algorithms (symmetric, asymmetric) and their use to ensure the security of information resources, public-key infrastructure (PKI), digital signature. |
| • *Mednarodne organizacije s področja informacijske varnosti:* SANS, ISF, NIST, ISACA, CERT, ISO, ENISA. | • *International organizations in the field of information security:* SANS, ISF, NIST, ISACA, CERT, ISO, ENISA. |
| • *Protokoli, standardi in ogrodja za zagotavljanje informacijske varnosti:* protokoli za varno komunikacijo (SSL, TLS, S/MIME, WEP, WPA), digitalni certifikati (X.509), sistem upravljanja informacijske varnosti (ISO 27001), kontrole zagotavljanja informacijske varnosti (ISO 27002), ogrodje Cobit. | • *Protocols, standards and frameworks for providing information security:* protocols for secure communications (SSL, TLS, S/MIME, WEP, WPA), digital certificates (X.509), information security management system (ISO 27001), information security controls (ISO 27002), Cobit framework. |
| • *Zakonodajni vidiki informacijske varnosti:* zakon o informacijski varnosti, zakon o elektronskih komunikacijah, zakon o varstvu osebnih podatkov, splošna uredba o varstvu podatkov (GDPR), zakon o | • *Regulatory aspects of information security:* Information Security Act, Electronic Communications Act, Personal Data Protection Act, General Data Protection Regulation (GDPR), Electronic Business |

| | |
|---|---|
| elektronskem poslovanju in elektronskem podpisu, kazenski zakonik.<br>• *Organizacijski vidiki informacijske varnosti:* določitev odgovornosti, razvoj varnostne strategije, razvoj varnostnih politik, načrtovanje, usmerjanje in izvajanje ukrepov, elementi kakovosti, informacijska varnostna kultura.<br>• *Obvladovanje tveganj:* identifikacija tveganj, metode za oceno tveganj, strategije nadzora tveganj (obramba, prenos, blaženje, sprejem), standard (ISO 27005).<br>• *Varnostne politike:* definicija, ključni elementi varnostne politike, razvoj varnostnih politik in pomen za zagotavljanje varnosti.<br>• *Specifične varnostne politike in primeri (ISO 27001)*: organizacijska varnost, varnost in nadzor nad sredstvi, osebje, fizična varnost, komunikacije in operativa, nadzor dostopa, razvoj in vzdrževanje programske opreme, poslovanje, skladnost z regulatornimi in tehničnimi zahtevami. | and Electronic Signature Act, Criminal Code.<br>• *Organisational aspects of information security:* defining responsibilities, developing a security strategy, developing security policies, planning, steering and implementing actions, quality elements, information security culture.<br>• *Risk management:* risk identification, risk assessment methods, risk control strategies (defend, transfer, mitigate, accept), standard (ISO 27005).<br>• *Security policies:* definition, basic security policy elements, policy development and their role in ensuring security.<br>• *Specific security policies and examples (ISO 27001):* organizational security, security and control over resources, personnel, physical security, communication and operations, access control, software development and maintenance, business, compliance with regulatory and technical requirements. |

**Temeljna literatura in viri/Readings:**

**Temeljna literatura/Basic literature**

- Prislan, K. in Bernik, I. (2019): Informacijska varnost in organizacije. Maribor: Univerzitetna založba Univerze v Mariboru.
- Whitman, M. E. in Mattord, H. J. (2022). Principles of Information Security. Boston: Cengage Learning.

**Priporočljiva literatura/Recommended literature**

- Rožanec, A. (2019). Elektronsko poslovanje. Novo mesto: Fakulteta za ekonomijo in informatiko, 2019.
- Egan, M. in Mather, T. (2005). Varovanje informacij: grožnje, izzivi in rešitve. Ljubljana: Pasadena.
- COBIT: https://www.isaca.org.
- Standard SIST ISO/IEC 27001: Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve.
- Standard SIST ISO/IEC 27002: Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri kontrolah informacijske varnosti.

| **Cilji in kompetence:** | **Objectives and competences:** |
|---|---|
| *Učna enota prispeva predvsem k razvoju naslednjih splošnih in specifičnih kompetenc:*<br>• usposobljenost za poglobljeno razumevanje računalništva in informatike, | *The learning unit mainly contributes to the development of the following general and specific competences:*<br>• competence for in-depth understanding of computer science and informatics, |

| | |
|---|---|
| • poznavanje in razumevanje procesov v tehniško-tehnološkem ter poslovnem okolju in sposobnost za njihovo analizo, sintezo in predvidevanje rešitev ter njihovih posledic,<br>• sposobnost definiranja, razumevanja in ustvarjalnega reševanja strokovnih izzivov na področjih računalništva in informatike,<br>• usposobljenost za permanentno spremljanje in presojo dogajanj na področju računalništva in informatike,<br>• usposobljenost za pridobivanje novih in poglabljanje pridobljenih strokovnih znanj računalništva in informatike,<br>• razvijanje poklicne identitete, profesionalne odgovornosti in etičnosti,<br>• pridobiti temeljno in aplikativno usposobljenost na področju računalništva in informatike, ki obsega osnovna teoretska in praktična znanja, bistvene za sodobno računalništvo in informatiko,<br>• poznavanje zmožnosti in omejitev informacijskih tehnologij,<br>• razumevanje in sposobnost umeščanja računalniških in informacijskih znanj na različna področja tehnike in druga strokovno relevantna področja (ekonomija, poslovanje, organizacijske vede itd.),<br>• izobraževanje uporabnikov s področja IKT. | • knowledge and understanding of processes in the technical-technological and business environment, as well as the ability for their analysis, synthesis and prediction of the solutions and their consequences,<br>• the ability to define, understand and creatively solve professional challenges in the fields of computer science and informatics,<br>• being qualified for continuous monitoring and assessment of events in the field of computer science and informatics,<br>• the ability to acquire new and deepen the acquired professional knowledge of computer science and informatics,<br>• developing occupational identity, professional responsibility and ethics,<br>• to acquire basic and applicative qualification in the field of computer science and informatics, which encompasses basic theoretical and practical knowledge essential for modern computer science and informatics,<br>• knowing the capabilities and limitations of information technologies,<br>• understanding and the ability to place computer and information knowledge into various fields of technics and other professionally relevant fields (economics, business, organizational sciences, etc.),<br>• educating users in the field of ICT. |

| **Predvideni študijski rezultati:** | **Intended learning outcomes:** |
|---|---|
| **Študent/Študentka:** | **Students:** |
| • razume pomen informacijske varnosti in temeljne pojme,<br>• pozna grožnje in ranljivosti različnih informacijskih virov,<br>• pozna tehnologije in postopke za zaščito virov pred tipičnimi grožnjami,<br>• pozna tehnologije in postopke za zmanjšanje tipičnih ranljivosti virov,<br>• razume delovanje simetričnih in asimetričnih kriptografskih algoritmov | • understand the importance of information security and the basic concepts,<br>• know the threats and vulnerabilities of different information resources,<br>• know technologies and procedures to protect resources against typical threats,<br>• know the technologies and procedures to reduce the typical vulnerabilities of resources, |

| | |
|---|---|
| ter njihovo uporabo pri zagotavljanju informacijske varnosti,<br>• pozna najpomembnejše organizacije s področja informacijske varnosti,<br>• pozna mednarodne standarde in ogrodja s področja informacijske varnosti,<br>• pozna ključne zakone za zagotavljanje informacijske varnosti, varstva podatkov, in varnega elektronskega poslovanja,<br>• zna analizirati stroške in koristi vlaganj v informacijsko varnost ter oceniti donosnost,<br>• je sposoben identifikacije varnostnih tveganj in grobe ocene stopnje tveganja,<br>• razume pomen in posledice pravilno definirane in ustrezno uveljavljanje varnostne politike,<br>• pozna zgradbo in postopek razvoja varnostne politike,<br>• sposoben je razviti preproste primere krovne (visokonivojske) in podrobne – specifične varnostne politike,<br>• je sposoben spremljati aktualno literaturo s tega področja in kritično ovrednotiti vsebino glede na usvojeno znanje,<br>• se (v okviru vaj) nauči oceniti stopnjo tveganja za različne informacijske vire konkretne organizacije ter smiselno predlagati ukrepe za obvladovanje tveganj (sprejetje, blažitev, prenos).<br>• se (v okviru vaj) izuri za pisanje specifičnih aktualnih varnostnih politik, npr. politika uporabe e-pošte, politika uporabe oddaljenega dostopa, politika rabe lastnih naprav (BYOD). | • understand the symmetric and asymmetric cryptographic algorithms and their use in providing information security,<br>• know the most important organizations in the field of information security,<br>• know the information security standards and frameworks,<br>• are familiar with key information security, data protection and secure electronic business acts,<br>• can analyze the costs and benefits of information security investments in and assess ROI,<br>• can identify risks and rough estimate risk levels.<br>• understand the importance and consequences of the properly defined and deployed security policy,<br>• know the structure and the development process of security policy,<br>• can develop simple examples of organizational (high-level) and detailed-specific security policies,<br>• can review the current literature in this field and to critically evaluate the content based on the established knowledge,<br>• learn (in the scope of laboratory exercises) to assess the level of risk for various information resources of a specific organization and to propose risk-management measures (acceptance, mitigation, transfer).<br>• learn (in the scope of laboratory exercises) to write specific security policies, e.g. e-mail policy, remote access policy, bring your own device (BYOD) policy. |

| **Metode poučevanja in učenja:** | **Learning and teaching methods:** |
|---|---|
| • *predavanja* z aktivno udeležbo študentov (razlaga, diskusija, vprašanja, primeri, reševanje problemov),<br>• *laboratorijske vaje:* v povezavi s predmetom (reševanje praktičnih problemov, uporaba programskih orodij),<br>• *seminarska naloga,*<br>• *samostojni študij.* | • *lectures* with active participation of students (explanation, discussion, questions, examples, problem solving),<br>• *laboratory work:* in connection with the course (solving practical problems, use of programming tools),<br>• *seminar paper*,<br>• *independent study*. |

| **Načini ocenjevanja:** | Delež (v %)<br>Weight (in %) | **Assessment:** |
|---|---|---|
| Načini:<br>• izpit<br>• izdelava, predstavitev in zagovor seminarske naloge<br><br>Ocenjevalna lestvica: ECTS. | 60 %<br>40 % | Types:<br>• exam<br>• preparation, presentation and defence of the seminar paper<br><br>Grading scheme: ECTS. |