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

Študijski program in stopnja Study programme and level	**Študijska smer Study field**	**Letnik Academic year**	**Semester 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 Lectures	**Seminar Seminar**	**Sem. vaje Tutorial**	**Lab. vaje Laboratory work**	**Teren. vaje Field work**	**Samost. delo 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. • Študent mora pred izpitom pripraviti in predstaviti seminarsko nalogo.	• The prerequisite for inclusion is enrolment in the second year of study. • 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. • *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. • *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. • *Organizacijski vidiki informacijske varnosti:* določitev odgovornosti, razvoj varnostne strategije, razvoj varnostnih politik, načrtovanje, usmerjanje in izvajanje ukrepov, elementi kakovosti, informacijska varnostna kultura. • *Obvladovanje tveganj:* identifikacija tveganj, metode za oceno tveganj, strategije nadzora tveganj (obramba, prenos, blaženje, sprejem), standard (ISO 27005). • *Varnostne politike:* definicija, ključni elementi varnostne politike, razvoj varnostnih politik in pomen za zagotavljanje varnosti. • *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. • *Organisational aspects of information security:* defining responsibilities, developing a security strategy, developing security policies, planning, steering and implementing actions, quality elements, information security culture. • *Risk management:* risk identification, risk assessment methods, risk control strategies (defend, transfer, mitigate, accept), standard (ISO 27005). • *Security policies:* definition, basic security policy elements, policy development and their role in ensuring security. • *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.
- 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.

Priporočljiva literatura/Recommended literature

- Whitman, M. E. in Mattord, H. J. (2017). Principles of Information Security. Boston: Cengage Learning.
- 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.

Cilji in kompetence:	**Objectives and competences:**
Učna enota prispeva predvsem k razvoju naslednjih splošnih in specifičnih kompetenc: • usposobljenost za poglobljeno razumevanje računalništva in informatike,	*The learning unit mainly contributes to the development of the following general and specific competences:* • 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, • sposobnost definiranja, razumevanja in ustvarjalnega reševanja strokovnih izzivov na področjih računalništva in informatike, • usposobljenost za permanentno spremljanje in presojo dogajanj na področju računalništva in informatike, • usposobljenost za pridobivanje novih in poglabljanje pridobljenih strokovnih znanj računalništva in informatike, • razvijanje poklicne identitete, profesionalne odgovornosti in etičnosti, • pridobiti temeljno in aplikativno usposobljenost na področju računalništva in informatike, ki obsega osnovna teoretska in praktična znanja, bistvene za sodobno računalništvo in informatiko, • poznavanje zmožnosti in omejitev informacijskih tehnologij, • razumevanje in sposobnost umeščanja računalniških in informacijskih znanj na različna področja tehnike in druga strokovno relevantna področja (ekonomija, poslovanje, organizacijske vede itd.), • 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, • the ability to define, understand and creatively solve professional challenges in the fields of computer science and informatics, • being qualified for continuous monitoring and assessment of events in the field of computer science and informatics, • the ability to acquire new and deepen the acquired professional knowledge of computer science and informatics, • developing occupational identity, professional responsibility and ethics, • 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, • knowing the capabilities and limitations of information technologies, • 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.), • educating users in the field of ICT.

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

ter njihovo uporabo pri zagotavljanju informacijske varnosti, • pozna najpomembnejše organizacije s področja informacijske varnosti, • pozna mednarodne standarde in ogrodja s področja informacijske varnosti, • pozna ključne zakone za zagotavljanje informacijske varnosti, varstva podatkov, in varnega elektronskega poslovanja, • zna analizirati stroške in koristi vlaganj v informacijsko varnost ter oceniti donosnost, • je sposoben identifikacije varnostnih tveganj in grobe ocene stopnje tveganja, • razume pomen in posledice pravilno definirane in ustrezno uveljavljanje varnostne politike, • pozna zgradbo in postopek razvoja varnostne politike, • sposoben je razviti preproste primere krovne (visokonivojske) in podrobne – specifične varnostne politike, • je sposoben spremljati aktualno literaturo s tega področja in kritično ovrednotiti vsebino glede na usvojeno znanje, • se (v okviru vaj) nauči oceniti stopnjo tveganja za različne informacijske vire konkretne organizacije ter smiselno predlagati ukrepe za obvladovanje tveganj (sprejetje, blažitev, prenos). • 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, • know the most important organizations in the field of information security, • know the information security standards and frameworks, • are familiar with key information security, data protection and secure electronic business acts, • can analyze the costs and benefits of information security investments in and assess ROI, • can identify risks and rough estimate risk levels. • understand the importance and consequences of the properly defined and deployed security policy, • know the structure and the development process of security policy, • can develop simple examples of organizational (high-level) and detailed-specific security policies, • can review the current literature in this field and to critically evaluate the content based on the established knowledge, • 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). • 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), • *laboratorijske vaje:* v povezavi s predmetom (reševanje praktičnih problemov, uporaba programskih orodij), • *seminarska naloga,* • *samostojni študij.*	• *lectures* with active participation of students (explanation, discussion, questions, examples, problem solving), • *laboratory work:* in connection with the course (solving practical problems, use of programming tools), • *seminar paper*, • *independent study*.

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