UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Varnost omrežij
Course title:	Network Security

Študijski program in stopnja **Study programme and level**	**Študijska smer** **Study field**	**Letnik** **Academic year**	**Semester** **Semester**
Kibernetska varnost, magistrski študijski program druge stopnje	-	Prvi	Prvi
The second cycle masters study programme Cyber Security	-	First	First

Vrsta predmeta / Course type	Obvezni / Obligatory
Univerzitetna koda predmeta / University course code:	5-KV-MAG-VOMR-2021-12-14

Predavanja **Lectures**	**Seminar** **Seminar**	**Vaje** **Tutorial**	**Klinične vaje** **work**	**Druge oblike študija**	**Samost. delo** **Individ. work**	**ECTS**
30	/	30	/	/	120	6

Nosilec predmeta / Lecturer:	doc. dr. Rok Bojanc

Jeziki / **Languages:**	**Predavanja / Lectures:**	Slovenski / Angleški
	Vaje / Tutorial:	Slovenski / Angleški

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**

Dodiplomska izobrazba iz IT smeri ali opravljeni diferencialni izpiti iz predmetov: • Uvoda v programiranje, • Informacijskih sistemov, • Operacijskih sistemov, • Računalniških omrežij in • Baz podatkov in modeliranja podatkov	Undergraduate education in IT or passed differential exams in the following subjects: • Introduction to programming, • Information systems, • Operating systems, • Computer Networks and • Databases and data modeling

Vsebina:	**Content (Syllabus outline):**
Uvod • Predstavitev načina dela pri predmetu in predstavitev osnovnih pojmov Omrežna arhitektura • Osnovne vrste in topologije omrežij, • komunikacijske naprave v omrežju • načini povezav, • brezžična omrežja TCP/IP in mrežni protokoli • Paketni prenosi, • TCP/IP protokol, • protokoli povezovalnega sloja (ethernet, 802.11, Bluetooth, arp), • protokoli omrežnega sloja (ip, icmp), • protokoli transportnega sloja (tcp, udp) Izvedba omrežja • Koncept odjemalec-strežnik, • peer-to-peer omrežja Omrežne storitve • Storitve naslavljanja in usmerjanja (dns, dhcp, nat, bgp), • storitve za izmenjavo podatkov (http, ftp, smtp, pop/imap, p2p) Grožnje in napadi v omrežju • Pregled pogostih vrst groženj, • motivi napadalcev, • ranljivosti omrežja in naprav, • možni napadi na posamezne točke omrežja Omrežna obramba • Osnove kriptografskih mehanizmov (simetrična in asimetrična kriptografija	Introduction • Presentation of the way of working on the course and presentation of basic concepts Network architecture • Basic types and topologies of networks, • communication devices in the network, • connection methods, • wireless networks TCP / IP and network protocols • Packet transmissions, • TCP / IP protocol, • link layer protocols (ethernet, 802.11, Bluetooth, arp), • network layer protocols (ip, icmp), • transport layer protocols (tcp, udp) Network implementation • Client-server concept, • peer-to-peer networks Network services • Addressing and routing services (dns, dhcp, nat, bgp), • data exchange services (http, ftp, smtp, pop / imap, p2p) Network threats and attacks • Overview of common types of threats, • motives of the attackers, • network and device vulnerabilities, • possible attacks on individual network points Network defense

enosmerne zgoščevalne funkcije, digitalni podpis, časovni žig, infrastruktura javnih ključev), • mehanizmi overjanja (gesla, dostopne pravice, biometrija, 801.x, Kerberos, RADIUS), • varnostne storitve in mehanizmi v različnih omrežnih slojih (IPsec, SSL/TLS, S/MIME, WS-security, SAML), • varnost brezžičnih omrežij, • požarni zidovi, • sistemi za odrivanje in preprečevanje vdorov Varovanje končnih točk • Navidezna zasebna omrežja (VPN) • protivirusna zaščita • zaščita pred nezaželeno pošto • varnost pri računalništvu v oblaku • varnost IoT Upravljanje varnosti omrežja • Standardizacija upravljanja varnosti omrežja (ISO 27001) • obvladovanje tveganj pri varnosti omrežja • varnostne politike • varnostni pregledi in penetracijska testiranja	• Basics of cryptographic mechanisms (symmetric and asymmetric cryptography of one-way compression function, digital signature, time stamp, public key infrastructure), • authentication mechanisms (passwords, access rights, biometrics, 801.x, Kerberos, RADIUS), • security services and mechanisms in different network layers (IPsec, SSL / TLS, S / MIME, WS-security, SAML), • security of wireless networks, • firewalls, • intrusion detection and intrusion prevention systems Endpoint protection • Virtual Private Networks (VPNs) • antivirus protection • spam protection • security in cloud computing • IoT security Network security management • Standardization of network security management (ISO 27001) • network security risk management • security policies • security auditing and penetration testing

Temeljni literatura in viri / Readings:

- Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Third Edition. Wiley Computer Publishing, 2020
- Bruce Schneier: Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. W. W. Norton & Compan, 2019
- Douglas E. Comer: Everything You Need to Know about Computer Networking and How the Internet Works (5th Edition). Chapman and Hall, 2018
- Douglas E. Comer: Internetworking with TCP/IP, Vol 1 (6th Edition). Prentice Hall, 2015
- Rok Bojanc, Borka Jerman-Blažič in Metka Tekavčič: Informacijska varnost v podjetniškem okolju: potrebe, ukrepi in ekonomika vlaganj. Ekonomska fakulteta, 2014

Cilji in kompetence:	**Objectives and competences:**

Splošne kompetence:

- Razumevanje pomena kibernetske varnosti.
- Sposobnost identifikacije kibernetskih varnostnih tveganj ter izdelave predlogov za ukrepanje in zaščito na osnovi identificiranih tveganj.
- Sposobnost pridobivanja, selekcije, analize informacij in zmožnost njihove interpretacije za celovito reševanje problemov, izzivov in incidentov s področja kibernetske varnosti.
- Poglobljeno razumevanje delovanja organizacijskih informacijskih sistemov, komponent in omrežij.
- Poznavanje uveljavljenih metodoloških pristopov za upravljanje varnosti sodobnih informacijskih sistemov in omrežij.
- Sposobnost iskanja podatkov in virov za potrebe upravljanja kibernetske varnosti.
- Sposobnost poslovnega komuniciranja, skupinskega dela in uporabe informacijskih tehnologij za namen zagotavljanja kibernetske varnosti.
- Sposobnost razvoja informacijskih varnostnih politik in sistemov upravljanja organizacije.
- Sposobnost fleksibilne uporabe pridobljenega znanja o kibernetski varnosti v praksi.
- Poznavanje pomena kakovosti in prizadevanje za kakovost strokovnega dela skozi avtonomnost, samoiniciativnost, (samo)kritičnost, (samo)refleksivnost in (samo)evalviranje.

Predmetno-specifične kompetence:

- Sposobnost ločevanja vrst omrežij
- Poznavanje standardov na področju arhitekture omrežij
- Poznavanje različnih topologij omrežij
- Razumevanje prenosa podatkov po različnih medijih
- Poznavanje tcp/ip modela

General competences:

- Understanding the importance of cyber security.
- The ability to identify cyber security risks and make proposals for action and protection based on identified risks.
- The ability to obtain, select, analyze information, as well as to interpret them to comprehensively solve problems, challenges and incidents in the field of cyber security.
- In-depth understanding of the functioning of organizational information systems, components and networks.
- Knowledge of established methodological approaches for security management of modern information systems and networks.
- The ability to find data and sources for the needs of cyber security management.
- The ability to do business communication, teamwork and use of information technology to ensure cyber security.
- The ability to develop information security policies and management systems of the organization.
- The ability of flexible usage of the acquired knowledge on cyber security in practice.
- Knowledge of the importance of quality and striving for the quality of professional work through autonomy, self-initiative, as well as (self-)criticism, (self-)reflection and (self-)evaluation.

Subject-specific competences:

- Ability to separate network types
- Knowledge of standards in the field of network architecture
- Knowledge of different network topologies
- Understanding data transfer across different media
- Knowledge of tcp / ip models

• Sposobnost praktične izvedbe lokalnega računalniškega omrežja • Poznavanje nevarnosti, ki se pojavljajo pri prenosu podatkov. • Poznavanje najpogostejših omrežnih varnostnih groženj • Poznavanje najpomembnejših protokolov in tehnologij za zagotavljanje varnosti v omrežju • Razumevanje delovanja požarnega zidu • Poznavanje navideznih zasebnih omrežij (vpn) in načine uvedbe • Razumevanje celostnega pristopa pri zagotavljanju varovanja omrežij • Poznavanje ključnih standardov na področju varovanja omrežij • Razumevanje pomena organizacijskega vidika zagotavljanja varnosti omrežij	• Ability to practically implement a local computer network • Knowledge of dangers that arise when transferring data. • Knowledge of the most common network security threats • Knowledge of the most important protocols and technologies for network security • Understanding how a firewall works • Knowledge of virtual private networks (vpn) and methods of implementation • Understanding an integrated approach to ensuring network security • Knowledge of key standards in the field of network security • Understanding the importance of the organizational aspect of ensuring network security

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: • Študenti bodo spoznali splošne zakonitosti komunikacij in omrežij, razumeli najpomembnejše protokole iz družine TCP/IP in spoznali ključne standarde na tem področju • Študenti bodo spoznali najpogostejše varnostne grožnje in varnostne tehnologije za zagotavljanje varnosti omrežij ter ključne standarde na področju. • Študenti bodo razumeli specifiko področja, potrebo po celostni obravnavi pri zagotavljanju varnosti omrežja ter potrebo po stalnem procesu za zagotavljanje varnosti omrežja. • Študenti se bodo naučili razumevanja in povezovanja teorije in prakse na področju varovanja omrežij, nadgradnje in povezovanja obstoječega znanja z novo pridobljenimi znanji s tega področja ter povezovanja upravljanja varnosti omrežja z drugimi procesi v organizaciji	Knowledge and understanding: • Students will learn the general laws of communications and networks, understand the most important protocols from the TCP/IP family and learn about key standards in this field • Students will learn about the most common security threats and security technologies to ensure network security and key standards in the field. • Students will understand the specifics of the field, the need for a comprehensive approach to ensuring network security and the need for an ongoing process to ensure network security. • Students will learn to understand and connect theory and practice in the field of network security, upgrade and integrate existing knowledge with newly acquired knowledge in this field and integrate network security management with other processes in the organization.

Metode poučevanja in učenja:	**Learning and teaching methods:**
• *Predavanja z aktivno udeležbo študentov* (razlaga, diskusija, vprašanja, primeri, reševanje problemov); • *Vaje*, kjer študentje na primerih ponovijo temeljne koncepte, predstavljene na predavanjih; • *Laboratorijske vaje*, kjer se študenti naučijo uporabljati ustrezne varnostne tehnologije in rešitve pred grožnjami in napadi na računalniška omrežja.	• *Lectures with active participations by the students* (explanation, discussion, questions, cases, problems solving); • *Tutorials*, where students will recall, reinforce, and shed light on the concepts and methods introduced at lectures; • *Lab work*, where students will learn to use appropriate security technologies and solutions against threats and attacks on computer networks.

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt):		Type (examination, oral, coursework, project):
Pisni izpit	60 %	Written Exam
Projektna naloga	40 %	Project assignment

Reference nosilca / Lecturer's references:

- BOJANC, Rok, JERMAN-BLAŽIČ, Borka. A quantitative model for information-security risk management. Engineering management journal. 2013, vol. 25, no. 3, str. 25-37. ISSN 1042-9247. [COBISS.SI-ID 26755879]
- BOJANC, Rok, JERMAN-BLAŽIČ, Borka, TEKAVČIČ, Metka. Managing the investment in information security technology by use of a quantitative modeling. Information processing & management. [Print ed.]. 2012, vol. 48, no. 6, str. 1031-1052. ISSN 0306-4573. DOI: 10.1016/j.ipm.2012.01.001. [COBISS.SI-ID 25578535]
- BOJANC, Rok, JERMAN-BLAŽIČ, Borka. Towards a standard approach for quantifying an ICT security investment. Computer standards & interfaces. [Print ed.]. 2008, vol. 30, no. 4, str. 216-222. ISSN 0920-5489. [COBISS.SI-ID 21277735]
- BOJANC, Rok, JERMAN-BLAŽIČ, Borka. An economic modelling approach to information security risk management. International journal of information management. [Print ed.]. 2008, vol. 28, no. 5, str. 413-422. ISSN 0268-4012. [COBISS.SI-ID 21486887]
- JERMAN-BLAŽIČ, Borka, MATSKANIS, Nikolaos, BOJANC, Rok. Semantic ontology design for a multi-cooperative first responder interoperable platform. Computing and informatics. 2016, vol. 35, no. 6, str. 1249-1276. ISSN 1335-9150. [COBISS.SI-ID 30268711]
- BOJANC, Rok, MÖREC, Barbara, TEKAVČIČ, Metka, JERMAN-BLAŽIČ, Borka. Model določitve optimalnega obsega vlaganj v informacijsko varnost. IB revija : za strokovna in metodološka vprašanja gospodarskega, prostorskega in socialnega razvoja Slovenije. [Slovenska tiskana izd.]. 2012, letn. 46, št. 3/4, str. 53-61, tabele, graf. prikazi. ISSN 1318-2803. [COBISS.SI-ID 21276134]

- BOJANC, Rok, JERMAN-BLAŽIČ, Borka. Quantitative model for economic analyses of information security investment in an enterprise information system. Organizacija : revija za management, informatiko in kadre. [Tiskana izd.]. nov.-dec. 2012, letn. 45, št. 6, str. 276-288, ilustr. ISSN 1318-5454. [COBISS.SI-ID 26317095]
- BOJANC, Rok. Kvantitativni model za upravljanje informacijskovarnostnih tveganj. Uporabna informatika. [Tiskana izd.]. apr./maj/jun. 2012, letn. 20, št. 2, str. 82-98, ilustr. ISSN 1318-1882. [COBISS.SI-ID 36236805]
- BOJANC, Rok, JERMAN-BLAŽIČ, Borka, TEKAVČIČ, Metka. Informacijska varnost v podjetniškem okolju : potrebe, ukrepi in ekonomika vlaganj. Ljubljana: Ekonomska fakulteta, 2014. Znanstvene monografije Ekonomske fakultete. ISBN 978-961-240-284-6. http://maksi2.ef.uni-lj.si/zaloznistvoslike/440/E-verzija_Monografija_Bojanc%20in%20soav_Informacijska%20varnost%20v%20podjetniskem%20okolju_feb2015.pdf. [COBISS.SI-ID 276133632]
- BOJANC, Rok. Analysis of research on e-invoicing in Slovenia = Analiza raziskav o izdajanju e-računov v Sloveniji. V: AŠKERC ZADRAVEC, Katarina (ur.). EECME conference 2021 : sustainable development in modern knowledge s : conference abstracts. Ljubljana: Ljubljana School of Business, 2021. [COBISS.SI-ID 67225603]
- BOJANC, Rok. Prototype of common IT-platform and test results. V: ITS Adriatic Multiport Gateway : technical workshop. Bruxelles: [s. n.]. 2013, str. 1-15. [COBISS.SI-ID 37142277]
- BOJANC, Rok. Analysis of e-invoicing as a driver for digital transformation. V: BELE, Darko (ur.), WEIS, Lidija (ur.). Sustainable development in a modern knowledge society : collective monograph. Ljubljana: Ljubljana School of Business, 2021. Str. 65-76, ilustr. ISBN 978-961-7110-02-9. [COBISS.SI-ID 70041603]