

KATALOG ZNANJA

1. IME PREDMETA

NAPREDNA OMREŽJA IN TEHNOLOGIJE

2. SPLOŠNI CILJI PREDMETA

Splošni cilji predmeta so:

- usposobiti se za stalno in aktivno spremljanje razvoja stroke s področja omrežij,
- pridobiti zavedanje o pomembnosti spremljanja novih tehnologij z vidika zagotavljanja kakovosti in varnosti,
- spodbujati kreativnost in inovativnost pri reševanju problemov,
- razviti kritično razmišljanje o vplivu sodobnih tehnologij na družbo in okolje.

Specifično strokovno usmerjeni cilji predmeta so:

- spoznati napredne omrežne tehnologije za uravnoteženo izkoriščanje virov omrežja,
- spoznati topologijo, protokole in organiziranost naprednih omrežij z vidika prometa,
- sodelovati z načrtovalci in uporabniki sodobnih informacijsko-komunikacijskih tehnologij in omrežij,
- poznati načine za preverjanje in merjenje delovanja kontrolnih mehanizmov,
- načrtovati in zagotavljati informacijsko-komunikacijsko varnost.

3. PREDMETNO SPECIFIČNE KOMPETENCE

Pri predmetu si študenti poleg generičnih pridobijo naslednje kompetence:

- načrtovanje NGN omrežij in topologije FMC,
- vzdrževanje in zagotavljanje kakovosti prometnih tokov,
- izvajanje prometnega inženiringa,
- uporabljanje sinhronizacije v paketnih omrežjih,
- uvajanje in načrtovanje varnostnih rešitev v komunikacijskih omrežjih in sistemih.

4. OPERATIVNI CILJI

INFORMATIVNI CILJI	FORMATIVNI CILJI
1. Načrtovanje NGN omrežij in topologije FMC	
<ul style="list-style-type: none">• spozna koncept NGN-omrežij;• pojasni načine prenosa govora prek IP-protokola v NGN-omrežjih (VoIP);• opiše različne koncepte prehoda in možne poti klasičnih omrežij v NGN-omrežje;• primerja naloge elementov NGN-omrežja in pripravi ustrezno arhitekturno rešitev;• spozna osnovni koncept prenosa govora v podatkovnih omrežjih;	<ul style="list-style-type: none">• argumentira prehod klasičnih omrežij v omrežja naslednje generacije (NGN);• načrtuje topologijo omrežnih elementov za storitve govora v fiksni in mobilni omrežjih.

<ul style="list-style-type: none"> • opiše arhitekturo in namen IMS-omrežja. 	
2. Upravljanje, vzdrževanje in zagotavljanje kakovosti prometnih tokov:	
<ul style="list-style-type: none"> • spozna sodobno organiziranost vzdrževanja omrežja; • spozna standarde, funkcije in delovanje administrativno-obratovalnih centrov; • spozna mehanizme za nadzor prometa in rešitve za obnovo delovanja ob nastalih okvarah (OAM v omrežjih Ethernet, MPLS, SDN, SD-WAN), podprto v standardih MEF; • razume zakonitosti paketnega transporta in prometne tokove; • razume mehanizme za označevanje paketov, klasifikacijo in razporejanje prometnih tokov; • razume delovanje mehanizmov za kontrolo delovanja omrežnih povezav in storitev; • utemelji cilje upravljanja prometa; • spozna funkcije upravljanja prometa in parametre QoS; • opiše prometne parametre; • spozna mehanizme za uveljavljanje prometnih parametrov z vidika zagotavljanja kakovosti. 	<ul style="list-style-type: none"> • izbere ustrezno storitev; • izmeri karakteristike prometnega toka; • izbere ustrezne prometne parametre za prenos določenih telekomunikacijskih storitev; • določi parametre kakovosti z vidika zagotavljanja kakovosti.
3. Izvajanje prometnega inženiringa	
<ul style="list-style-type: none"> • spozna posamezne faze prometnega inženiringa in pomembne naloge; • razume pomen samodejnega zaščitnega preklapljanja (APS); • razume načine za zaščito prometnih tokov; • ponazori rešitve prometnega inženiringa. 	<ul style="list-style-type: none"> • oceni pomen in načine razporejanja prometnih tokov v podomrežjih; • uporabi optimalni način zaščite storitve v omrežju; • načrtuje izvedbo posameznih aktivnosti za izvajanje prometnega inženiringa.
4. Uporabljanje sinhronizacije v paketnih omrežjih:	
<ul style="list-style-type: none"> • opiše razloge in potrebe po sinhronizaciji v paketnih omrežjih; • klasificira načine paketne in linijske sinhronizacije; • pozna tehnične možnosti za sinhronizacijo v paketnih omrežjih. 	<ul style="list-style-type: none"> • izbere primeren način sinhronizacije v omrežju.
5. Uvajanje in načrtovanje varnostnih rešitev v komunikacijskih omrežjih in sistemih:	
<ul style="list-style-type: none"> • razume pomen informacijskokomunikacijske varnosti prenosa podatkov; • pojasni vidike informacijsko-komunikacijske varnosti; • spozna koncepte varovanja informacij; • pojasni načine varovanja informacij v omrežjih; 	<ul style="list-style-type: none"> • oceni varnostne zmožnosti varnostnih naprav; • uporabi ustrezna orodja in postopke za analizo komunikacijske varnosti; • izvede spremembe za nadgradnjo informacijsko-komunikacijske varnosti;

<ul style="list-style-type: none"> • spozna koncepte varovanja komunikacijsko informacijskih sistemov; • pozna postopke za zaščito informacijsko-komunikacijske varnosti (omrežij, omrežnih elementov in zaščite podatkov v komunikaciji). • razloži uporabo varnostnih mehanizmov in varnostne rešitve v različnih tipih omrežij; • spozna načine proaktivnega zagotavljanja informacijske varnosti (orodja, sisteme, procese); • spozna različne metode testiranja ranljivosti in vdornega testiranja; • opiše različne metode za zaščito zaupnosti in varnosti v komunikacijskih omrežjih, sistemih in aplikacijah. • predstavi varnostne rešitve v različnih tipih omrežij. 	<ul style="list-style-type: none"> • uporabi ustrezno varnostno rešitev v procesu načrtovanja informacijske varnosti; • oceni ranljivost različnih omrežij in aplikacij (OWASP); • oceni varnostne zmožnosti varnostnih naprav; • izvede testiranje ranljivosti omrežja; • izbere ustrezno varnostno rešitev glede na ranljivost in ogroženost komuniciranja; • načrtuje varnostne rešitve komunikacijskih omrežij.
6. Upravljanje in nadziranje informacijsko-komunikacijske varnosti :	
<ul style="list-style-type: none"> • razume načine proaktivnega zagotavljanja informacijske varnosti (orodja, sisteme, procese); • spozna osnove etičnega hekinga s posameznimi orodji (zunanji in notranji pregled); • pozna OSINT (informacije iz javnih virov); • pozna delovanje odzivnih centrov za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (CERT skupin) ter obveščanje v primeru najdenih ranljivosti. 	<ul style="list-style-type: none"> • oceni ranljivost različnih omrežij, naprav, aplikacij; • izvede varnostni pregled zunanjega in notranjega omrežja. • se ustrezno odzove glede na varnostne dogodke.

5. OBVEZNOSTI ŠTUDENTOV IN POSEBNOSTI V IZVEDBI

Število kontaktnih ur: 76 (48 ur predavanj, 28 ur laboratorijskih vaj). Število ur samostojnega dela študenta: 74 (študij literature, priprave na laboratorijske vaje, študij navodil in tehnične dokumentacije, izdelava izdelka oziroma storitve z zagovorom).