KATALOG ZNANJA

1. IME PREDMETA

VAROVANJE INFORMACIJSKIH SISTEMOV (VIS)

2. SPLOŠNI CILJI

Splošni cilji predmeta so:

- razvijanje samoiniciativnosti, ustvarjalnosti in natančnosti,
- uporaba pisnih virov in informacijsko komunikacijske tehnologije pri reševanju problemov,
- razvijanje sposobnosti za samostojno spremljanje razvoja stroke in uvajanja novosti v praksi,
- razvijanje pripravljenosti za sodelovanje pri skupinski izvedbi nalog,
- razvijanje zavesti o pomenu organizacijske kulture.

3. PREDMETNO-SPECIFIČNE KOMPETENCE

Pri predmetu si študent poleg generičnih pridobi naslednje kompetence:

- razvija spretnosti za praktično delo pri varovanju in zaščiti informacijskih sistemov,
- zna uporabljati strokovni jezik s področja varovanja in zaščite informacijskih sitemov,
- zna poiskati in uporabljati strokovno literaturo in vire s področja varovanja in zaščite informacijskih sistemov,
- presoja ukrepe na področju varovanja in zaščite informacijskega sistema v kontekstu učinkovitosti celotnega poslovnega sistema,
- uporablja standarde in priporočila na področju varovanja informacijsko - komunikacijskih tehnologij,
- se usposobi za svetovanje uporabniku pri izbiri rešitev za realizacijo varnega informacijskega sistema,
- se usposobi za sodelovanje pri projektiranju varnosti in zaščite informacijskih sistemov,
- sistematsko nadzira delovanje informacijskega sistema in ukrepa v smislu zagotavljanja neprekinjenega delovanja.

4. OPERATIVNI CILJI

INFORMATIVNI CILJI Študent:	FORMATIVNI CILJI Študent:
PREGLED PODROČJA VAROVANJA INFORMACIJ	
• spozna osnovne pojme s področja varovanja informacij, • spozna področje varovanja informacij, • razume izzive varovanja informacij.	• je sposoben opredeliti pojem *varovanje informacij*, • zna predstaviti področje varovanja informacij in izzive s tega področja.
VARNOSTNI SISTEM	
• spozna elemente varnostnega sistema, • razume cilje uvedbe varovalnih ukrepov, • spozna nivoje zagotavljanja varnosti v organizaciji (fizični, logični, organizacijski).	• je sposoben opredeliti osnovne elemente varnostnega sistema in njihove medsebojne odnose, • oceni nivo varnosti, • zna predstaviti in razložiti konkretni primer varnostnega sistema.
VAROVANJE INFORMACIJSKIH SISTEMOV	
• spozna razliko med varovanjem informacij in varovanjem informacijskih sistemov, • zna opredeliti pojem varovanje informacijskih sistemov,	• zna izdelati oceno občutljivosti IS, • zna izdelati varnostni načrt skozi vse faze življenskega cikla IS.

• spozna pomen načrtovanja varnosti v življenskem krogu informacijskega sistema, • razume vključevanje varnosti v življenski cikel sistema, • spozna organizacijo varovanja IS, • razume vloge in odgovornosti pri varovanju IS, • spozna varnostne kontrole.	
UPRAVLJANJE VARNOSTNIH TVEGANJ	
• spozna različne vrste ranljivosti in groženj, • se seznani z različnimi metodologijami izvedbe analize tveganj, • se seznani z osnovnimi načini upravljanja tveganj.	• zna uporabiti metodologije analize tveganj v praksi, • kritično oceni in ovrednoti varnostno tveganje določenega informacijskega sistema, • zna poiskati ustrezna nadzorstva za zmanjšanje tveganja.
SISTEM UPRAVLJANJA VAROVANJA INFORMACIJ (Information Security Management System)	
• razume sistem upravljanja varovanja informacij, • pozna mednarodne standarde na področju varovanja informacij, • se seznani z upravljanjem dokumentacije sistema upravljanja varovanja informacij, • se seznani z upravljanjem varnostnih incidentov, • se seznani z nadzorstvi standarda ISO/IEC 27001, • spozna načine preverjanja uspešnosti delovanja sistema upravljanja varovanja informacij, • se seznani s standardom BS 25999.	• zna uporabljati varnostne standarde kot pripomoček pri delu, • zna preveriti uspešnost delovanja varnostnega sistema, • zna izpeljati postopek vodenja reševanja varnostnega incidenta, • zna pripraviti splošen načrt neprekinjenosti poslovanja.
ZAGOTAVLJANJE VARNOSTI V INFORMACIJSKIH SISTEMIH	
• razume pomen vdora v informacijski sistem, • spozna vrste zlonamernih programov, • razume mehanizme delovanja in širjenja zlonamernih programov, • spozna načine zaščite pred zlonamernimi programi, • spozna avtomatska orodja za zaščito IS, • pozna metode obnavljanja informacijskega sistema po napadu, • razume delovanje požarnega zidu, • razume namen overjanja pri uporabi informacijskih sistemov, • spozna različne načine overjanja, • pozna politiko gesel, • razume pomen kriptiranja podatkov, • pozna vrste in metode kriptiranja pri prenosu podatkov, • razume mehanizem elektronskega podpisa, • spozna mehanizme kriptiranja datotek.	• izvede namestitev in nastavitve zaščitne opreme pred zlonamernimi programi, • preizkusi delovanje zaščite pred zlonamernimi programi, • uporabi različne algoritme za kriptiranje podatkov, • samostojno nastavi zaščito proti neželeni e-pošti, • zna obravnavati varnostne dogodke, • zna pregledati sistemske dnevnike.
PSIHOLOGIJA VAROVANJA	
• spozna vlogo človeka v varnostnem sistemu, • spozna pojem *socialni inženiring*, • spozna metode socialnega inženiringa,	• je sposoben prepoznati delovanje socialnih inženirjev, • se zna zaščititi pred socialnim inženiringom.

• spozna načine zaščite proti socialnemu inženiringu, • zna opredeliti pojem *socialni inženiring*, • se seznani s primeri socialnega inženiringa v praksi.	

5. OBVEZNOSTI ŠTUDENTOV in POSEBNOSTI V IZVEDBI

Število kontaktnih ur: 80 ((40 ur predavanj, 24 ur seminarskih vaj, 16 ur laboratorijskih vaj)
Število ur samostojnega dela: 100