KATALOG ZNANJA

1. IME PREDMETA

VARNOST IN ZAŠČITA

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 študenti poleg generičnih pridobijo naslednje kompetence:

- razvijajo spretnosti za praktično delo pri varovanju in zaščiti informacijskih sistemov,
- znajo uporabljati strokovni jezik s področja varovanja in zaščite informacijskih sitemov,
- znajo poiskati in uporabljati strokovno literaturo in vire iz področja varovanja in zaščite informacijskih sistemov,
- presojajo ukrepe na področju varovanja in zaščite informacijskega sistema v kontekstu učinkovitosti celotnega poslovnega sistema,
- uporabljajo standarde in priporočila na področju varovanja informacijsko-komunikacijskih tehnologij,

- se usposobijo za svetovanje uporabniku pri izbiri rešitev za realizacijo varnega informacijskega sistema,
- se usposobijo za sodelovanje pri projektiranju varnosti in zaščite informacijskih sistemov,
- sistematsko nadzirajo delovanje informacijskega sistema in ukrepajo v smislu zagotavljanja neprekinjenega delovanja.

4. OPERATIVNI CILJI

INFORMATIVNI CILJI	FORMATIVNI CILJI
Študent:	Študent:
1. VARNOST V RAZVOJNI FAZI PROJEKTA INFORMACIJSKEGA SISTEMA	
• spozna pomen in problem varnosti v fazi projektiranja informacijskega sistema, • razume vrednotenje informacijske varnosti v kontekstu zagotavljanja neprekinjenega poslovanja poslovnega sistema.	
2. VARNOSTNO TVEGANJE	
• spozna organizacijo sistema varovanja informacij, • razčleni vrste varnostnih nesreč, • spozna nivoje varnostnega tveganja, • se seznani z osnovnimi načini upravljanja s tveganji.	• s spleta pridobi ažurno informacijo o aktualnih nevarnostih informacijskih sistemov, • kritično oceni in ovrednoti varnostno tveganje za svoje okolje.
3. SISTEM VAROVANJA INFORMACIJ – ISMS (Information Security Management System)	
• razume sistem za upravljanje z informacijsko varnostjo v poslovnem subjektu, • se seznani z mednarodnimi standardi na področju varnosti informacijskih sistemov, • pozna pomen in vrste varnostne dokumentacije ISMS • razlikuje pristope različnih varnostnih politik.	
4. ZLONAMERNI PROGRAMI	
• razume pomen vdora v informacijski sistem,	• izvede namestitev in nastavitve zaščitne

• spozna vrste zlonamernih programov, • razume mehanizme delovanja in širjenja zlonamernih programov, • spozna načine zaščite pred zlonamernimi programi, • pozna metode obnavljanja informacijskega sistema po napadu • razume delovanje požarnega zidu.	opreme pred zlonamernimi programi, • preizkusi delovanje zaščite pred zlonamernimi programi, • samostojno izvede obnovitev napadenega računalnika po okužbi z zlonamernim programom.
5. VARNOST V INFORMACIJSKIH SISTEMIH	
• razume namen overjanja pri uporabi informacijskih sistemov, • spozna različne načine overjanja, • pozna politiko gesel, • razume tehnologijo zaupnih sistemov (Trusted System).	• vzpostavi gesla za uporabnike po pravilih za kreiranje gesel in izdela dokumentacijo opravljenega dela.
6. KRIPTIRANJE	
• razume pomen kriptiranja podatkov, • pozna vrste in metode kriptiranja pri prenosu podatkov, • razume mehanizem elektronskega podpisa, • spozna mehanizme kriptiranja datotek.	• uporabi različne algoritme za kriptiranje podatkov.
7. NAVIDEZNA PRIVATNA OMREŽJA (VPN)	
• spozna osnove navideznih privatnih omrežij (VPN), • spozna prednosti in slabosti povezave navideznih privatnih omrežij (VPN).	• vzpostavi navidezno privatno povezavo (VPN), analizira njeno delovanje in poroča o ugotovitvah.
8. PREVAJANJE OMREŽNIH NASLOVOV (NAT)	
• spozna pomen prevajanja omrežnih naslovov (NAT), • osvoji osnovne nastavitve za prevajanje omrežnih naslovov (NAT) in delo z njim.	
9. PROGRAMSKA OPREMA ZA ARHIVIRANJE	
• spozna pomen arhiviranja v informacijskih sistemih, • spozna delovanje programov za arhiviranje, • seznani se z različnimi načini arhiviranja na različnih platformah operacijskih sistemov.	• uporabi programe za arhiviranje v okolju Linux in v okolju Windows.

5. OBVEZNOSTI ŠTUDENTOV IN POSEBNOSTI V IZVEDBI

Število kontaktnih ur: 72 ur (36 ur predavanj, 36 ur vaj).
Število ur samostojnega dela: 78 ur (42 ur študij literature, 36 ur seminarska naloga).
Skupaj 150 ur dela študenta (5 KT).
Obvezna je prisotnost na vajah, izdelava in predstavitev seminarske naloge ter pisni izpit.