KATALOG ZNANJA

1. IME PREDMETA

VARNOST RAČUNALNIŠKIH SISTEMOV

2. SPLOŠNI CILJI PREDMETA

Splošni cilji predmeta so:

- razviti samoiniciativnosti, ustvarjalnosti in natančnosti;
- naučiti se uporabiti pisne vire in informacijsko-komunikacijske tehnologije pri reševanju problemov;
- razviti sposobnost za samostojno spremljanje razvoja stroke in uvajanja novosti v praksi;
- razviti pripravljenosti za sodelovanje pri skupinski izvedbi nalog;
- razviti zavesti o pomenu organizacijske kulture;
- usposobiti se za povezovanje pridobljenih znanj z znanji iz drugih strokovnih področij;
- usposobiti se za kontinuirano in aktivno spremljanje razvoja stroke s področja varovanja računalniških sistemov.

Specifično strokovno usmerjeni cilji so:

- pridobiti spretnosti za praktično delo pri varovanju in zaščiti računalniških sistemov;
- ukrepati na področju varovanja in zaščite računalniških sistemov v kontekstu učinkovitosti celotnega poslovnega sistema;
- uporabljati standarde in priporočila na področju varovanja informacijsko-komunikacijskih tehnologij;
- svetovati uporabniku pri izbiri rešitev za realizacijo varnih računalniških sistemov;
- razumeti ranljivosti sistemov upravljanja informacijske varnosti;
- sodelovati pri projektiranju varnosti in zaščite računalniških sistemov;
- nadzirati delovanja računalniških sistemov in ukrepanje v smislu zagotavljanja neprekinjenega delovanja;
- uporabljati strokovno literaturo in vire s področja varovanja in zaščite računalniških sistemov.

3. PREDMETNOSPECIFIČNE KOMPETENCE

Pri predmetu si študenti poleg generičnih pridobijo naslednje kompetence:

1. ocenjevanje in uporabljanje varnosti v računalniških sistemih;
2. implementacija zaščite pred zlonamernimi programi;

3. izvajanje varnosti v računalniških sistemih;
4. uporabljanje sistemov upravljanja varovanja informacij (ang. Information Security Management System);
5. vrednotenje varnostnega tveganja.

4. OPERATIVNI CILJI

INFORMATIVNI CILJI	FORMATIVNI CILJI
1. Ocenjevanje in uporabljanje varnostni v računalniških sistemih:	
• opredeli, kaj je informacijski sistem z opredelitvijo njegovih glavnih komponent; • definira triado informacijske varnosti; • pojasni koncepte na visoki ravni v zvezi z orodji za informacijsko varnost; • pojasni razliko med varovanjem informacij in varovanjem računalniških sistemov; • razume pojem varovanje računalniških sistemov; • zamisli si načrt varnosti v življenjskem krogu informacijskega sistema; • pojasni vključevanje varnosti v življenjski cikel sistema; • opredeli organizacijo varovanja računalniških sistemov; • utemelji vloge in odgovornosti pri varovanju računalniških sistemov; • razloži namen overjanja pri uporabi računalniških sistemov; • pojasni različne načine overjanja; • razume politiko gesel; • razloži tehnologijo zaupnih sistemov (ang. Trusted System).	• izvede vzpostavitev gesel za uporabnike po pravilih za kreiranje gesel in izdela dokumentacijo opravljenega dela; • izdela oceno občutljivosti računalniškega sistema; • izdela varnostni načrt skozi vse faze življenjskega cikla računalniškega sistema.
2. Implementacija zaščite pred zlonamernimi programi:	
• razloži pomen vdora v informacijski sistem; • razlikuje vrste zlonamernih programov; • opredeli mehanizme delovanja in širjenja zlonamernih programov; • loči različne načine zaščite pred zlonamernimi programi; • pojasni metode obnavljanja informacijskega sistema po napadu;	• izvede namestitev in nastavitve zaščitne opreme pred zlonamernimi programi; • izvede preizkus delovanja zaščite pred zlonamernimi programi; • izvede obnovitev napadenega računalnika po okužbi z zlonamernim programom.

• pojasni delovanje požarne pregrade.	
3. Izvajanje varnosti v računalniških sistemih:	
• razlikuje različne načine zaščite pred zlonamernimi programi; • razloži avtomatska orodja za zaščito računalniških sistemov; • opredeli namen overjanja pri uporabi računalniških sistemov; • ovrednoti različne načine overjanja; • razume politiko gesel; • razloži pomen kriptiranja podatkov; • loči različne vrste in metode kriptiranja pri prenosu podatkov; • opredeli mehanizem elektronskega podpisa; • razume mehanizme kriptiranja datotek.	• uporabi različne algoritme za kriptiranje podatkov; • izvede nastavitve zaščite proti neželeni e-pošti; • izvede pregled sistemskih dnevnikov.
4. Uporabljanje sistemov upravljanja varovanja informacij (ang. Information Security Management System):	
• pojasni sistem upravljanja varovanja informacij; • opredeli mednarodne standarde na področju varovanja informacij; • zamisli si upravljanje dokumentacije sistema upravljanja varovanja informacij; • razume upravljanje varnostnih incidentov; • razloži standarda ISO/IEC 27001; • razlikuje različne načine preverjanja uspešnosti delovanja sistema upravljanja varovanja informacij; • razloži standard BS 25999.	• uporabi varnostne standarde za upravljanje varovanja informacij; • izvede preverbo uspešnost delovanja varnostnega sistema; • izvede postopek vodenja reševanja varnostnega incidenta.
5. Vrednotenje varnostnega tveganja:	
• oceni različne vrste ranljivosti in groženj; • analizira administratorska opravila, ki se nanašajo na varovanje in zaščito računalniškega sistema; • razlikuje različne metodologije izvedbe analize tveganj; • opredeli osnovne načine upravljanja tveganj; • razloži organizacijo sistema varovanja informacij; • razčleni vrste varnostnih nesreč; • razume ravni varnostnega tveganja;	• izdela kritično oceno in ovrednoti varnostno tveganje določenega informacijskega sistema; • išče informacije na internetu za ustrezna nadzorstva za zmanjšanje tveganja; • na spletu poišče in uporabi ažurno informacijo o aktualnih nevarnostih računalniških sistemov; • izdela kritično oceno in ovrednoti varnostno tveganje za svoje okolje.

• zamisli si osnovne načine upravljanja s tveganji; • ovrednoti ustreznost delovanja elementov varovanja podatkov (npr. nadziranje uporabe sredstev, postopek diferenčnega/postopnega varnostnega kopiranja, delovanje mreže pomnilniških naprav).	

5. OBVEZNOSTI ŠTUDENTOV IN POSEBNOSTI V IZVEDBI

Število kontaktnih ur: 75 (40 ur predavanj, 35 ur laboratorijskih vaj).

Število ur samostojnega dela študenta: 150 (študij literature, delo z besedilom, študij primerov, reševanje in analiza nestandardiziranih vprašalnikov in anket, priprava pisnih besedil, predstavitev, izvedba javnega nastopa, igre vlog …).