

KATALOG ZNANJA

1. IME PREDMETA

UPRAVLJANJE INFORMACIJSKE VARNOSTI

2. SPLOŠNI CILJI

Splošni cilji predmeta so:

- naučiti postopkov rednega varovanja občutljivih podatkov v podjetju;
- predstaviti pomen sistemov upravljanja informacijske varnosti - ISMS;
- razviti zavest o etičnih aspektih uporabe podatkovnega rudarjenja;
- usposobiti za razreševanje težav, kritično mišljenje, analitično razmišljanje, sprejemanje odločitev, učinkovito komunikacijo ter razviti digitalno pismenost;
- naučiti načrtovanja in določanja prioritet, samoupravljanja, samostojnega učenja ter samorefleksije;
- usposobiti za projektno vodenje.

Specifično strokovno usmerjeni cilji so:

- načrtovati celovite sisteme upravljanja informacijske varnosti - ISMS za rabo v podjetjih;
- obvladati in uporabiti mednarodne standarde (npr. ISO 27001:2013, i. d.) za ISMS;
- izvajati redne nadzore in izboljševanje ISMS v podjetjih, da se omogoči centraliziran pristop k varovanju podatkov.

3. PREDMETNO SPECIFIČNE KOMPETENCE

Pri predmetu študenti poleg generičnih pridobijo naslednje kompetence:

1. analiziranje temeljnih principov upravljanja informacijske varnosti;
2. vrednotenje postopkov implementacije in vzdrževanja sistemov upravljanja informacijske varnosti – ISMS;
3. ocenjevanje ranljivosti sistemov upravljanja informacijske varnosti;
4. analiziranje prednosti in slabosti implementacije standardov kakovosti za sisteme upravljanja informacijske varnosti.

4. OPERATIVNI CILJI

INFORMATIVNI CILJI	FORMATIVNI CILJI
1. Analiziranje temeljnih principov upravljanja informacijske varnosti	
<ul style="list-style-type: none"> • definira pojem sistemov upravljanja informacijske varnosti – ISMS ter njihov pomen za varnost in uspešno delovanje podjetij; • razčleni pomen načel (npr. zasebnost, dovoljenja, varnost informacij, upravljanje z dolžnostmi, minimalen dostop, i. d.); • definira tveganja (vpliv, verjetnost, ranljivosti ter grožnje) ter upravljanje s tveganji (npr. prenos, mediacija, sprejem, izogibanje, i. d.); • ovrednoti prednosti učinkovitega ISMS za podjetja. 	<ul style="list-style-type: none"> • izdelava navodila zahtevanih korakov za vzpostavitev in vzdrževanje ISMS za izbrano podjetje, vključno z zahtevami standarda ISO 27001:2013. • sestavi seznam deležnikov, ki bi se potencialno zanimali za implementacijo ali izboljšavo ISMS.
2. Vrednotenje postopkov implementacije in vzdrževanja sistemov za upravljanje informacijske varnosti – ISMS	
<ul style="list-style-type: none"> • analizira elemente ter procese za vzpostavitev in vzdrževanje ISMS; • definira zahteve deležnikov, postopek ocenjevanja tveganj, načrtovanja odzivov na grožnje, izdelavo pravil, • oceni kriterije revizija ISMS (interna, eksterna) ter možnosti za nadzor delovanja ter za nadgradljivost posameznih elementov ISMS; • ovrednoti kriterije za učinkovit postopek implementacije ISMS. 	<ul style="list-style-type: none"> • izdelava poročila o delovanju ali postopku implementacije ISMS v podjetju.
3. Ocenjevanje ranljivosti sistemov upravljanja informacijske varnosti	
<ul style="list-style-type: none"> • opiše kriterije za določevanje ranljivosti sistemov upravljanja informacijske varnosti; • analizira prednosti in slabosti uporabe ISMS v podjetjih ter izpostavi pogoste težave; • ovrednoti značilnosti dokumentacijo ISMS ter izpostavi šibkosti in predlaga izboljšave. 	<ul style="list-style-type: none"> • oceni izbrani ISMS in predstavi morebitne pomanjkljivosti sistema.

4. Analiziranje prednosti in slabosti implementacije standardov kakovosti za sisteme upravljanja informacijske varnosti

<ul style="list-style-type: none">• definira namen in vsebino standardov ISO 27000 ter klavzule ISO 27001:2013.• analizira razmerje med ISO 27001:2013 in vzpostavitev ISMS v določenih podjetjih.• ovrednoti prednosti in slabosti s certifikatom.	<ul style="list-style-type: none">• izdelava poročila zahtev deležnikov za določevanje obsega ISMS ter ovrednoti pravila, vloge ter odgovornosti v podjetju, za implementacijo ukrepov proti tveganju.
---	--

5. OBVEZNOSTI ŠTUDENTOV IN POSEBNOSTI V IZVEDBI

Število kontaktnih ur: 80 ur (40 ur predavanj, 40 ur laboratorijskih vaj).

Število ur samostojnega dela študenta: 180 (študij literature, delo z besedilom, študij primerov, priprava pisnih besedil za izdelavo poročil in navodil ...).