KATALOG ZNANJA

1. IME PREDMETA

INFORMATIKA IN VARNOST

2. SPLOŠNI CILJI

Splošni cilji predmeta so:

- predstaviti pomen varnosti informacijskih tehnologij v podjetjih ter organizacijah,
- predstaviti cilje varovanja premoženja podjetja;
- predstaviti vrste fizičnih ter digitalnih ranljivosti v podjetju ter upravljanje s tveganji v podjetju ali organizaciji;
- razviti medosebne veščine ter strokovno izražanje;
- razviti sposobnost razreševanja težav, kritičnega mišljenja, analitičnega razmišljanja, sprejemanja odločitev, digitalno pismenost ter kreativnost;
- usposobiti za načrtovanje in določanje prioritet, samoupravljanja, ter samorefleksije,
- razviti zavest o strokovnem področju ter o vplivu tehnologije na vsakdanji potek dela.

Specifično strokovno usmerjeni cilji so:

- obvladati delovanje varnostne opreme za računalniška omrežja ter preventivne ukrepe proti ranljivostim;
- poznati posledice vdorov na delovanje podjetja ter pristope za učinkovit odziv na vdore;
- postavljati pravila, smernice za varnost, za boljšo prepoznavo ranljivosti ter vdorov v podjetje;
- upravljati z avtorizacijami dostopa do informacijske tehnologije, o regulaciji uporabe ter o določanju varnostnih pravil in postopkov;
- načrtovati računalniška omrežja, preverjati omrežne naslove, vzpostavljati območja upravljanja s podatki;
- obvladati in namestiti navidezna zasebna omrežja VPN, požarne zidove, antivirusne programe ter sisteme za zaznavanje vdorov;
- uporabiti oddaljen dostop za pregled ranljivosti ter izpopolnjevanje varnostnih predpisov in organizacijske presoje.

3. PREDMETNO SPECIFIČNE KOMPETENCE

Pri predmetu študenti poleg generičnih pridobijo naslednje kompetence:

1. uporabljanje informacijskih virov in osnovnih komponent informacijske tehnologije ter komuniciranje preko računalniških omrežij;
2. uporabljanje programske opreme za urejanje besedil, preglednic in predstavitev;
3. ocenjevanje varnostnih tveganj informacijske tehnologije;
4. opredeljevanje varnostnih rešitev informacijske tehnologije;
5. pregledovanje celovitosti obvladovanja varnosti informacijske tehnologije v podjetjih;
6. upravljanje varnosti informacijske tehnologije v podjetjih.

4. OPERATIVNI CILJI

INFORMATIVNI CILJI	FORMATIVNI CILJI
1. Uporabljanje informacijskih virov in osnovnih komponent informacijske tehnologije ter komuniciranje preko računalniških omrežij	
● definira pomen in vlogo rabe posameznih sestavnih delov informacijske tehnologije v podjetju ter našteje elemente in specifike uporabe določene programske opreme; ● opiše postopek izvajanja osnovnega podatkovnega komuniciranja; ● definira in opiše strukturo računalniških omrežij; ● analizira postopek dela z uporabniškimi programi; ● razčleni možnosti za uporabo operacijskih sistemov ter programske opreme v podjetjih; ● analizira osnovne varnostne funkcije za zaščito informacijskih sistemov; ● utemelji osnove programskega jezika XHTML; ● ovrednoti postopek varnega iskanja informacij na spletu ter ustvarjanja povezav do aktualnih vsebin; ● oceni postopek zagotavljanja varnosti informacijske tehnologije v podjetju.	● izdela analizo osnovnih funkcij informacijskih naprav; ● uporabi bližnjice za določeno programsko opremo ter izvede osnovne funkcije v operacijskem sistemu; ● implementira funkcije za premik, brisanje in kopiranje datotek in map ter izvede postopek tiskanja; ● uporabi osnovne funkcije programske opreme, operacijskega sistema ter orodij za komunikacijo; ● ustvari datoteko z osnovnimi ukazi v programskem jeziku za označevanje XHTML.

2. Uporabljanje programske opreme za urejanje besedil, preglednic in predstavitev	
● definira rabo programske opreme za obdelavo besedil, preglednic in predstavitev; ● opiše postopek strukturiranja delovnih zvezkov ter uporabo kompleksnih formul v preglednicah; ● analizira dodatna orodja posamezne programske opreme ter implementira sloge za oblikovanje besedila in nastavi delovno okolje v programski opremi; ● definira postopek ustvarjanja poročil z uporabo tabel in grafikonov; ● razčleni možnosti za uporabo naprednih funkcij programske opreme ter načinov ogledovanja ter postavitve diapozitivov in vstavljanje animacij; ● ovrednoti postopek upravljanja s podatki (npr. razvrščanje, samodejno in napredno filtriranje v preglednicah, i. d.).	● izvede postopek pisanja, oblikovanja ter tiskanja besedila z uporabo programske opreme; ● implementira tabele, slike in matematične izraze v besedilo; ● implementira samodejno ustvarjanje kazal, obrazcev, opomb ter drugih sklicev in povezav v dokument; ● izdela elektronsko preglednico, predstavi podatke v obliki grafikona ter izdela digitalno predstavitev vsebine; ● implementira orodja za iskanje ter optimizacijo podatkov; ● izvede funkcijo digitalnega podpisovanja v dokumentu.
3. Ocenjevanje varnostnih tveganj informacijske tehnologije	
● loči pojma zaščita in varnost računalniškega sistema ter definira cilje in principe zaščite računalniškega sistema; ● analizira administratorska opravila, ki se nanašajo na varovanje in zaščito računalniškega sistema; ● opredeli varnostne grožnje in napade na računalniški sistem; ● našteje tveganja pri varnosti informacijske tehnologije; ● analizira procesne podatke o delovanju informacijsko-komunikacijske opreme in storitev (npr. skripte, Prometheus in drugi programi za analizo); ● definira vrste tveganj pri varnosti ob koriščenju informacijske tehnologije v podjetjih ● opiše splošno prisotna tveganje pri koriščenju informacijske tehnologije;	● izdela načrt ter tehnično poročilo o metodi za ocenjevanje in ravnanje z varnostnimi tveganji informacijske tehnologije. ● dodeljuje pravice za dostop do elementov datotečnega sistema v različnih operacijskih sistemih na nivoju uporabnika ter skupin; ● izdela najmanj tri fizične in digitalne varnostne ukrepe, ki zagotavljajo integriteto varnosti informacijske tehnologije v podjetju; ● namesti in uporablja programsko opremo za zaščito računalniškega sistema na različnih operacijskih sistemih (npr. požarni zid, antivirusni programi, i. d.);

● razloži funkcionalnost varnostnega kopiranja podatkov, postopkov pregledovanja (podatkov ter omrežij); ● utemelji delovanje prostranih omrežij WAN, intraneta ter dostopovnih sistemov; ● analizira neavtorizirane načine uporabe informacijske tehnologije, neavtorizirano odstranjevanje ali kopiranje podatkov ter kode v sistemu; ● razčleni postopke implementacije varnosti informacijske tehnologije v podjetjih ● primerja različne vrste fizične škode ali uničenje opreme ter škodo v programski kodi informacijske tehnologije; ● presodi ustreznost delovanja elementov varovanja podatkov (npr. nadziranje uporabe sredstev, postopek diferenčnega/postopnega varnostnega kopiranja, delovanje mreže pomnilniških naprav, i. d.); ● ovrednoti delovanje stabilnost delovanja varnostnih ukrepov v podjetju;	● izdela predstavitev o raznih varnostnih kršitvah in o njihovem vplivu na operativno delovanje podjetja.
4. Opredeljevanje varnostnih rešitev informacijske tehnologije	
● opredeli načine vrednotenja varnostnih rešitev za informacijsko tehnologijo; ● utemelji delovanje varne mrežne infrastrukture (npr. vrednotenje preverjanja omrežnih naslovov NAT, območij upravljanja z podatki DMZ ter požarnih zidov, i. d.); ● opiše delovanje podatkovnih centrov ter procese delovanja (npr. virtrualizacija, delovanje varnih protokolov za prenose, varno usmerjanje večprotokolnih komutacij label MPLS, i. d.); ● analizira kriterije za učinkovito delovanje omrežja (npr. nastavitve RAID, Main/Standby, Dual LAN, uravnovešenost spletnega strežnika, i. d.); ● analizira ranljivosti v varnosti informacijske tehnologije (npr. datoteke z	● izdela območje upravljanja s podatki, statičnim IP ter NAT ter izdela poročilo o izboljšavi varnosti določenega omrežja. ● izdela tehnično poročilo o potencialnih posledicah neustreznih nastavitev programske opreme za VPN tretjih oseb ter pravil požarnega zidu na delovanje varnosti informacijske tehnologije;

zapisi, digitalni odtis, delovanje algoritmov za podatkovno rudarjenje, termin honeypots, i. d.); ● opredeli prednosti implementacije nadzornih sistemov omrežij za namen podpore ter vzdrževanja.	
5. Pregledovanje celovitosti obvladovanja varnosti informacijske tehnologije v podjetjih	
● pojasni postopke ocenjevanja tveganj pri koriščenju informacijske tehnologije; ● opredeli mehanizme za nadzor varnosti informacijske tehnologije za podjetja in organizacije; ● ugotovi bistvene značilnosti postopkov nadzora nad presojo varnosti, sprememb pri upravljanju omrežij; ● utemelji pomen načrtov za stalno delovanje varnostnih sistemov v podjetju ter načrtov za ponovno vzpostavitev delovanja v primeru večjih težav; ● napove posledice izgube podatkov ter kritično osvetli odgovornosti zaposlenih, glede na Zakon o varstvu osebnih podatkov ter standard ISO 31000; ● analizira proces upravljanja ter varovanja podatkov v podjetju; ● izpostavi podrobnosti varnostnih ukrepov ter vpliv neskladnosti z internimi smernicami; v podjetju ● ovrednotiti možne vplive na varnost v podjetju s pomočjo varnostne presoje informacijske tehnologije. ● oceni možnosti za usklajevanje smernic v podjetju ter strategije za varnost informacijske tehnologije.	● izdela poročilo o primernih predpisih za varnost informacijske tehnologije v podjetju (npr. kriteriji za dostop do sistemov, vrste fizičnega varovanja – biometrične naprave, magnetne kartice ter druge metode za preprečevanje kraje, i. d.); ● izdela predstavitev o vrednotenju metodologije obvladovanja tveganj ISO 31000 ter uporabo standarda za varnost informacijske tehnologije.
6. Upravljanje varnosti informacijske tehnologije v podjetjih	
● opredeli napredne možnosti za nadzor in upravljanje varnosti informacijske tehnologije v podjetjih; ● primerja pravila za dostop do raznih sistemov kot so e-mail, brskalniki, uporaba in nameščanje programske	● opredeli napredne možnosti za nadzor in upravljanje varnosti informacijske tehnologije v podjetjih; ● primerja pravila za dostop do raznih sistemov kot so e-mail,

opreme, fizični dostop ter dostop tretjih oseb; ● razčleni metode varovanja ter definira kodeks dobrih praks pri upravljanju varnosti informacijske tehnologije; ● navede vloge deležnikov za ustrezno implementacijo predlogov in varnostne presoje. ● izpostavi pomen informiranja sodelavcev o njihovih odgovornostih za varnost v podjetju ter pomen preverjanja njihovega razumevanja na ustrezno določenih intervalih; ● ovrednoti nadzor nad presojo varnostnih tveganj ter skladnost z varnostnimi postopki in standardi (npr. ISO/IEC 17799:2005, i. d.); ● ovrednoti ustreznost orodij za varnost informacijske tehnologije, ki so v uporabi v skladu s pravili in smernicami v podjetju. ● izdela tehnično poročilo o pravilih za varnost informacijske tehnologije v podjetju. ● izdela načrt osnovnih komponent za ponovno vzpostavitev delovanja ter zaščito podatkov v podjetju in utemelji razloge za implementacijo.	brskalniki, uporaba in nameščanje programske opreme, fizični dostop ter dostop tretjih oseb; ● razčleni metode varovanja ter definira kodeks dobrih praks pri upravljanju varnosti informacijske tehnologije; ● navede vloge deležnikov za ustrezno implementacijo predlogov in varnostne presoje. ● izpostavi pomen informiranja sodelavcev o njihovih odgovornostih za varnost v podjetju ter pomen preverjanja njihovega razumevanja na ustrezno določenih intervalih; ● ovrednoti nadzor nad presojo varnostnih tveganj ter skladnost z varnostnimi postopki in standardi (npr. ISO/IEC 17799:2005, i. d.); ● ovrednoti ustreznost orodij za varnost informacijske tehnologije, ki so v uporabi v skladu s pravili in smernicami v podjetju. ● izdela tehnično poročilo o pravilih za varnost informacijske tehnologije v podjetju. ● izdela načrt osnovnih komponent za ponovno vzpostavitev delovanja ter zaščito podatkov v podjetju in utemelji razloge za implementacijo.

5. OBVEZNOSTI ŠTUDENTOV IN POSEBNOSTI V IZVEDBI

Število kontaktnih ur: 60 ur (15 ur predavanj, 15 ur seminarskih vaj 30 ur laboratorijskih vaj).
Število ur samostojnega dela študenta: 150 (študij literature, delo z besedilom, študij primerov, priprava pisnih besedil, preglednic, tehničnih poročil in predstavitev …)