

KATALOG ZNANJA

1. Ime modula: Varovanje informacijskih sistemov

2. Usmerjevalni cilji

Dijak bo zmožen:

- povezovati teoretična znanja s področja varovanja podatkov v informatiki s konkretnimi nalogami,
- uporabljati zakonodajo s področja varovanja podatkov in varovanja osebnih podatkov,
- izvajati naloge varovanja podatkov v informacijskih sistemih, internetu, računalniških omrežjih,
- razvijati znanje na področju informacijskih sistemov, računalništva in programske opreme, kriptografije,
- uporabljati programsko opremo s področja identifikacije osebja,
- ustrezno komunicirati s strankami, naročniki, sodelavci,
- vzpostavljati stike z ljudmi, komunicirati situaciji primerno in reševati probleme,
- uporabljati ukrepe zaščite podatkov pred nepooblaščenimi osebami,
- nadgrajevati znanje z dodatnim izobraževanjem in izpopolnjevanjem,
- zagotavljati kakovost lastnega dela in storitev,
- voditi evidence in dokumentacijo,
- prepoznati in pravilno reagirati ob pojavu socialnega inženiringa.:-

3. Poklicne kompetence

OZNAKA	VAROVANJE INFORMACIJSKIH SISTEMOV
VIS1	Varovanje podatkov v informatiki
VIS2	Varovanje računalniških omrežij
VIS3	Strokovno komuniciranje
VIS 4	Socialni inženiring

4. Operativni cilji

VIS1 - Varovanje podatkov v informatiki

INFORMATIVNI CILJI	FORMATIVNI CILJI
Dijak: <ul style="list-style-type: none">▪ pozna ustrezna teoretična izhodišča s področja varovanja podatkov v informatiki;▪ se seznani z ustrezno zakonodajo na področju varovanja podatkov, varovanja osebnih podatkov, državnih skrivnosti, zaupnih in strogo zaupnih dokumentov;▪ pozna delovanje računalniških omrežij, izmenjave podatkov v	Dijak: <ul style="list-style-type: none">▪ uporabi teoretična znanja s področja varovanja podatkov in sodeluje pri reševanju konkretnih problemov;▪ uporabi zakonodajo s področja varovanja podatkov, osebnih podatkov in se zaveda pomena tajnosti zaupnih podatkov;

<p>elektronski obliki, programske opreme, kriptografije in varovanja podatkov v elektronski obliki;</p> <ul style="list-style-type: none"> ▪ se seznanj s programsko opremo ter napravami za identifikacijo osebja; ▪ pozna vlogo policije in drugih upravnih organov v primeru kaznivega dejanja, dogodka ali škodnega primera; ▪ se seznanj z raznovrstnimi operacijskimi sistemi in njihovim načinom delovanja ter najrazličnejšo programsko opremo; ▪ se seznanj z delovanjem mrežnih strežnikov in zaščito podatkov na strežniku; ▪ se izpopolnjuje na področju programske opreme; ▪ pozna osnove delovanja računalnikov; ▪ se seznanj z ukrepi v primeru nepooblaščenega dostopa do podatkov (vdora v sistem); ▪ se seznanj z delovanjem brezžičnih računalniških omrežij in varovanjem podatkov v njih; ▪ obvlada osnove pomoči uporabnikom računalniške programske opreme. 	<ul style="list-style-type: none"> ▪ razvija znanja na področju delovanja računalniških omrežij, programske opreme, varovanja podatkov; ▪ v primeru nepooblaščenega dostopa do tajnih podatkov ukrepa skladno z zakonom, obvesti varnostno-nadzorni center in pristojne organe; ▪ uporablja različne računalniške operacijske sisteme in ustrezno programsko opremo; ▪ uporablja programsko opremo in naprave za identifikacijo osebja – biometrični podatki; ▪ uporablja programsko opremo za mrežne strežnike; ▪ skrbi za brezhibno delovanje računalnikov, ▪ upošteva zakone, postopke in navodila v primeru nepooblaščenega vstopa v računalniški sistem; ▪ uporablja brezžična računalniška omrežja in jih zaščiti pred drugimi osebami; ▪ namesti programsko opremo; ▪ namesti brezžično omrežje; ▪ svetuje uporabnikom programske opreme.
---	---

VIS2 - Varovanje računalniških omrežij

INFORMATIVNI CILJI	FORMATIVNI CILJI
<p>Dijak:</p> <ul style="list-style-type: none"> ▪ pozna ustrezna teoretična znanja s področja računalniških omrežij; ▪ pozna programske in strojne zahteve za izvedbo računalniških omrežij; ▪ se seznanj s protokoli, ki omogočajo delovanje računalniških omrežij; ▪ pozna varovanje računalniških omrežij in informacijskih sistemov; 	<p>Dijak:</p> <ul style="list-style-type: none"> ▪ uporabi teoretična znanja v praksi, na primerih iz vsakdanjega življenja; ▪ uporabi programsko in strojno opremo za izvedbo računalniških omrežij; ▪ namesti in aktivira ustrezne računalniške protokole, ki omogočajo delovanje mreže; ▪ računalniško mrežo zaščiti tako, da imajo dostop do podatkov le pooblašчени uporabniki;

<ul style="list-style-type: none"> ▪ razume delovanje skupne rabe datotek in tiskalnikov ter možnost nepooblaščenega dostopa do fizičnih materialov; ▪ se seznani z elektronskim prenosom podatkov po računalniških mrežah in s shranjevanjem podatkov pri uporabnikih; ▪ pozna nevarnosti računalniških virusov, ter drugih škodljivih programov; ▪ pozna načine za odstranitev računalniških virusov in drugih škodljivih programov; ▪ pozna načine za arhiviranje podatkov; ▪ pozna načine za reševanje poškodovanih oziroma izbrisanih podatkov; ▪ pozna načine in metode za pomoč uporabnikom. 	<ul style="list-style-type: none"> ▪ prepreči možnost tiskanja dokumentov na oddaljenih tiskalnikih, če imajo dostop do natisnjenih dokumentov nepooblašcene osebe; ▪ podatke prenaša v elektronski obliki po najrazličnejših medijih ter omrežjih, pri tem se zaveda pomembnosti varovanja podatkov; ▪ uporablja programsko opremo za odstranjevanje rač. virusov in drugih škodljivih programov, pri tem se zaveda nevarnosti virusov in izgube podatkov; ▪ pred nevarnimi opravili na računalniku arhivira podatke; ▪ v primeru izbrisa pomembnih podatkov ali dokumentov jih zna obnoviti; ▪ svetuje in nudi pomoč uporabnikom, ki niso večji uporabe računalnikov v skladu s pooblastili.
--	--

VIS3 - Strokovno komuniciranje

INFORMATIVNI CILJI	FORMATIVNI CILJI
<p>Dijak:</p> <ul style="list-style-type: none"> ▪ pozna ustrezna komunikacijska sredstva in metode, pravila ustnega in pisnega komuniciranja; ▪ prepozna varnostno sumljive osebe, okoliščine in varnostno dogajanje; ▪ pozna osebne in druge uradne dokumente; ▪ opiše metode in postopke za reševanje varnostnega dogodka; ▪ pozna delovanje komunikacijskih sredstev; ▪ se seznani s strokovno terminologijo in poslovnim bontonom. 	<p>Dijak:</p> <ul style="list-style-type: none"> ▪ uporabi ustrezna komunikacijska sredstva in metode; ▪ daje primerna navodila, vzpostavlja stike, usmerja, opozarja, obvešča, daje osnovne informacije, opazuje, nadzira, piše poročila in zapisnike; ▪ opiše varnostno dogajanje; ▪ deluje v skladu s svojimi pristojnostmi, izvaja postopke ugotavljanja istovetnosti oseb; ▪ o varnostnem dogodku obvesti pristojne organe in naročnike, varnostno-nadzorni center; ▪ daje navodila in omogoči evakuacijo ljudi in premoženja iz ogroženega območja ▪ preverja komunikacijska sredstva; ▪ uporablja strokovno terminologijo in poslovni bonton.

--	--

VIS 4 – Socialni inženiring

INFORMATIVNI CILJI	FORMATIVNI CILJI
Dijak: <ul style="list-style-type: none">▪ pozna pojem socialni inženiring;▪ se seznani s tehnikami socialnega inženiringa;▪ pozna načine zaščite pred socialnim inženiringom.	Dijak: <ul style="list-style-type: none">▪ prepozna socialni inženiring in njegovo delovanje;▪ prepozna tehnike socialnega inženiringa in njihov vpliv na varnost in delovanje informacijskih sistemov;▪ uporablja primerno tehniko in tehnologijo za zaščito pred socialnim inženiringom.