

# Bezbednost podataka i informacija 2011/2012

## Teorijska pitanja:

### 1. Upotreba informacionih tehnologija

1. Šta se podrazumeva pod pojmom računarska pismenost?
2. Šta obuhvata ciklus obrade informacija?
3. Kakva je razlika između medijuma i uređaja za skladištenje?
4. Navedite osnovnu poddelu softvera.
5. Šta se podrazumeva pod SISTEMSKIM SOFTVEROM? Koje dve osnovne grupe on obuhvata?
6. Navedite pet osnovnih kategorija računara.
7. Navedite osnovne karakteristike grafičkog korisničkog interfejsa.
8. Šta se podrazumeva pod APLIKATIVNIM SOFTVEROM?
9. Koje dva grupe tehnologija predstavljaju osnov savremenog informatičkog okruženja?
10. Šta se podrazumeva pod pojmom sistem?
11. Koje elemente poseduje svaki sistem?
12. Šta se podrazumeva pod misijom sistema?
13. Šta se podrazumeva pod organizacionom strukturom sistema?
14. Šta se podrazumeva pod funkcionalnom strukturom sistema?
15. Šta se podrazumeva pod informacionom strukturom sistema?
16. Šta se podrazumeva pod upravljačkom strukturom sistema?
17. Kako se, na osnovu opšte teorije informacija, može definisati INFORMACIJA?
18. Šta se podrazumeva pod pojmom informacioni sistem?
19. Šta se podrazumeva pod pojmom automatizovani informacioni sistem?
20. Navedite osnovne faze u evoluciji INFORMACIONIH SISTEMA.
21. Šta se podrazumeva pod pojmom SISTEMI ZA OBRADU PODATAKA?
22. Šta se podrazumeva pod pojmom KLASIČNI UPRAVLJAČKI INFORMACIONI SISTEMI?
23. Šta se podrazumeva pod pojmom INTERAKTIVNI ON-LINE UPRAVLJAČKI INFORMACIONI SISTEMI?
24. Šta se podrazumeva pod pojmom INFORMACIONI SISTEMI ZA PODRŠKU ODLUČIVANJU?
25. Šta se podrazumeva pod pojmom INTELIGENTNI INFORMACIONI SISTEMI?
26. Navedite osnovne izazove savremenih tehnologija i koncepata u domenu projektovanja informacionih sistema.
27. Navedite dva osnovna tipa računarskih mreža.
28. Koja je osnovna karakteristika lokalnih računarskih mreža?
29. Koja je osnovna karakteristika računarskih mreža na širokom prostoru?
30. Navedite dva osnovna tipa lokalnih računarskih mreža.
31. Navedite bar 4 od 6 uloga koje serveri mogu imati u sklopu lokalne računarske mreže sa serverima.
32. Šta se podrazumeva pod mrežnom topologijom?
33. Navedite osnovne topologije računarskih mreža.
34. Koja je osnovna osobina MAGISTRALNIH računarskih mreža? Koji je osnovni problem u ovakvim mrežama?
35. Koja je osnovna osobina ZVEZDASTIH računarskih mreža? Šta se smatra njihovom lošom osobinom?

36. Navedite dobre osobine zvezdastih računarskih mreža.
37. Koja je osnovna osobina PRSTENASTIH računarskih mreža? Šta se smatra njihovom lošom osobinom?
38. Navedite osnovne komunikacione tehnologije koje se koriste u mrežama na širokom prostoru.
39. Navedite osnovne osobine paketskih mreža.
40. Koje slojeve obuhvata ISO-OSI referentni model?
41. Kakva je uloga sloja APLIKACIJE ISO-OSI modela?
42. Kakva je uloga sloja PREZENTACIJE ISO-OSI modela?
43. Kakva je uloga sloja SESIJE ISO-OSI modela?
44. Kakva je uloga TRANSPORTNOG sloja ISO-OSI modela?
45. Kakva je uloga MREŽNOG sloja ISO-OSI modela?
46. Kakva je uloga sloja VEZE PODATAKA ISO-OSI modela?
47. Kakva je uloga FIZIČKOG sloja ISO-OSI modela?
48. Kojih šest emelenata čine osnove Interneta?
49. Šta se podrazumeva pod PROTOKOLIMA i šta oni definišu?
50. Navedite pet slojeva Internet protokola.
51. Šta se podrazumeva pod pojmom ADRESIRANJE na Internetu?
52. Šta predstavlja IP-ADRESA?
53. Koja je osnovna uloga DNS sistema?
54. Objasnite pojam URL-a.
55. Objasnite pojam URL ADRESE.
56. Koje delove podesuje URL-ADRESA?
57. Koja tri dela čine mrežniu strukturu?
58. Šta obuhvata mrežna grana?
59. Šta obuhvata jezgro mreže?
60. Koja je osnovna razlika između mreže sa komutacijom kanala i mreže sa komutacijom paketa?
61. U čemu se sastoji razlika između standardnog teksta i hiperteksta?
62. Šta je HTML?
63. Koja su dva elementa neophodna za uspostavljanje www servisa?
64. Šta se podrazumeva pod pojmom web-server?
65. Šta se podrazumeva pod pojmom web-kljijent?
66. Navedite ELEMENTE PREKO KOJIH KOMUNICIRAJU WEB-KLIJENT I WEB-SERVER.
67. Šta se podrazumeva pod pojmom HTTP?
68. Kako se nazivaju dokumenti u koje se smeštaju informacije na Web-u?
69. Navedite četiri faze u kojima se obavlja jedna HTTP transakcija.
70. Zbog čega se HTTP protokol smatra asimetričnim?
71. Kakva je razlika između pojmova Internet i WEB?
72. Šta obuhvata organizacija dokumenata na Web-u?
73. Šta se podrazumeva pod kreiranjem web-dokumenata?
74. Šta se podrazumeva pod kreirenjem internih i eksternih hipertekst linkova između Web-dokumenaza?
75. Šta se podrazumeva pod dizajniranjem i organizovanjem strukture Web-sajta?
76. Šta se podrazumeva pod pojmom NAVIGACIJE u sklopu pretraživanja Web-dokumenata?
77. Šta seu Web-pretraživači? Navedite najpoznatije Web-pretraživače.

78. Navedite osnovne načine na koje je moguće ostvariti pristup Web-stranicama uz oslonac na Web-pretraživače.
79. Šta se podrazumeva pod pojmom servisa elektronske pošte? Na kom nivou Internet protokola se ovaj servis nalazi?
80. Od čega se sastoji elektronska poruka?
81. Šta predstavlja zaglavlje elektronske poruke?
82. Šta se nalazi u sklopu tela elektronske poruke?
83. Koji uslovi moraju biti zadovoljeni da bi se mogao koristiti servis elektronske pošte?
84. Navedite osnovne delove standardne e-mail adrese.
85. Šta predstavlja ime korisnika u sklopu e-mail adrese?
86. Šta predstavlja ime domena u sklopu e-mail adrese i na šta ono upućuje?
87. Koja dva elementa poseduje e-mail server?
88. Kakva je uloga SMTP - servera?
89. Kakva je uloga POP3 – servera?
90. U čemu se sastoji razlika između POP3 i IMAP protokola?
91. Šta se podrazumeva pod listama slanja i koja je njihova uloga u sklopu e-mail klijenta?

## **2. Profil kriminalca u domenu informacionih tehnologija (može biti dopunjeno)**

92. Navedite osnovne razlike između amatera, profesionalnih kriminalca i hakera.
93. Šta se podrazumeva pod pojmom kiber-terorizam?
94. Koje su osnovne karakteristike profila kiber-teroriste?
95. Navedite osnovne načine suprotstavljanja kiber-terorizmu.

## **3. Zaštita od zloupotreba informacionih tehnologija**

96. Zlatna pitanja zaštite informacionog ambijenta.
97. Šta se podrazumeva pod objektima zaštite u informacionom ambijentu? Navedite bar 8 (osam) tipičnih objekata zaštite u sklopu informacionog ambijenta.
98. Šta se podrazumeva pod pojmom pretnja?
99. Šta se podrazumeva pod pojmom posledica kompromitovanja informacione bezbednosti? Navedite osnovne primere posledica.
100. Šta se podrazumeva pod pojmom mere zaštite?
101. Kako se mere zaštite mogu klasifikovati u skladu sa prirodnim osobinama koje ih karakterišu?
102. Navedite osnovne normativne mere zaštite. U koju grupu one spadaju?
103. Koje su osnovne karakteristike pravnih mera zaštite?
104. Navedite osnovne karakteristike organizacionih mera zaštite.
105. Šta obuhvataju kadrovske mere zaštite?
106. Šta se podrazumeva pod pojmom politike zaštite?
107. Koji su osnovni ciljevi upravljanja rizikom?
108. Da li se rizici ugrožavanja informatičke bezbednosti mogu eliminisati? Obrazložiti odgovor.
109. Navedite osnovne strategije odgovora na informacione pretnje. Šta obuhvata strategija IZBEGAVANJA RIZIKA?
110. Navedite osnovne strategije odgovora na informacione pretnje. Šta obuhvata strategija PRIHVATANJA RIZIKA?
111. Navedite osnovne strategije odgovora na informacione pretnje. Šta obuhvata strategija PRENOŠENJA RIZIKA?
112. Navedite osnovne strategije odgovora na informacione pretnje. Šta obuhvata strategija KONTROLISANJA RIZIKA?
113. Šta obuhvataju fizičko-tehnički aspekti zaštite i koje tri grupe mera one obuhvataju?

114. Šta obuhvata zaštita magnetnih nosilaca podataka?
115. Šta obuhvataju mere elektronskog obezbeđenja?
116. Šta se podrazumeva pod merama LOGIČKE ZAŠTITE u sklopu informacionih sistema?
117. Koje osobine mora zadovoljiti informacija da bi je smatrali POUZDANOM?
118. Navedite pet osnovnih principa koji doprinose pouzdanosti sistema. Šta podrazumeva princip BEZBEDNOSTI?
119. Navedite pet osnovnih principa koji doprinose pouzdanosti sistema. Šta podrazumeva princip POVERLJIVOSTI?
120. Navedite pet osnovnih principa koji doprinose pouzdanosti sistema. Šta podrazumeva princip PRIVATNOSTI?
121. Navedite pet osnovnih principa koji doprinose pouzdanosti sistema. Šta podrazumeva princip INTEGRITETA ODBADE?
122. Navedite pet osnovnih principa koji doprinose pouzdanosti sistema. Šta podrazumeva princip RASPOLOŽIVOSTI?
123. Na šta se usredsređuje model bezbednosti baziran na blagovremenom odgovoru? Koja tri vida mera on zahteva?
124. Na čemu se bazira ideja dubinske odbrane?
125. Šta je cilj preventivnih mera zaštite? Koja dva povezana mehanizma oni uključuju?
126. Na šta je usmerena provera autentičnosti? Na osnovu koja tri elementa se ona može obaviti?
127. Na šta je usmerena provera ovlašćenja?
128. Koja četiri zahteva mora da zadovolji efektivna lozinka?
129. Koji je osnovni mehanizam implementacije provere ovlašćenja?
130. Koji element predstavlja prvi nivo preventivne zaštite u sklopu modela dubinske zaštite?
131. Šta predstavlja drugi nivo preventivnih mehanizama zaštite u sklopu modela dubinske zaštite?
132. Šta obuhvata kontrola udaljenog pristupa? Na kom nivou preventivne zaštite se ona nalazi?
133. Šta se smešta u sklopu demilitarizovane zone mrežne infrastrukture?
134. Šta obuhvata osnaživanje servera? Na kom nivou preventivne zaštite se ono nalazi?
135. Koji je poslednji sloj u sklopu dubinske odbrane? Koja je njegova osnovna karakteristika?
136. Objasnite razliku između ŠIFRIRANJA i KODIRANJA.
137. Šta je i šta obuhvata KRIPTOLOGIJA?
138. Kakva je razlika između KRIPTOGRAFIJE i KRIPTOANALIZE?
139. Navedite osnovnu poddelu sistema šifriranja?
140. Na čemu se zasniva princip ŠIFRIRANJA?
141. Na čemu se zasniva princip KODIRANJA?
142. Koja dva principa se najčešće koriste kod klasičnih sistema šifriranja? Šta podrazumeva princip šifriranja SIPSTITUCIJOM?
143. Navedite osnovne primerke supstitucionih šifarskih sistema? Na kom principu se bazira Cezarova šifra?
144. Koja dva principa se najčešće koriste kod klasičnih sistema šifriranja? Šta podrazumeva princip šifriranja TRANSFORMACIJOM?
145. Kakva je razlika između monoalfabetskih i polialfabetskih šifarskih sistema.
146. Navedite osnovne slabosti monoalfabetskih šifarskih sistema. Koji se metod koristi za razbijanje monoalfabetskih substitucionih šifarskih sistema?
147. Na čemu se zasniva polialfabetska supstitucija?
148. Koja je osnovna karakteristika šifarskih sistema koji koriste TRANSPOZICIJU?

149. Koja tri vida transpozicije se koriste u šifarskim sistemima sa transpozicijom? Obrazložite princip proste transpozicije.
150. Koja tri vida transpozicije se koriste u šifarskim sistemima sa transpoticijom? Obrazložite princip tablične transpozicije.
151. Koja tri vida transpozicije se koriste u šifarskim sistemima sa transpoticijom? Obrazložite princip transpozicije ključem.
152. Koja četiri elementa karakterišu moderne kriptografske metode?
153. Ka koje dve osnovne grupe se dele moderne kriptografske metode?
154. Kakva je razlika između simetričnih i asimetričnih modernih kriptografskih metoda?
155. Navedite osnovne probleme SIMETRIČNIH KLJUČEVA?
156. Navedite osnovne prednosti ASIMETRIČNIH KLJUČEVA? Šta je njihov nedostatak?
157. Navedite najznačajnije moderne kriptografske metode.
158. U koju grupu šifarskih sistema, sa aspekta ključeva, spadaju DES i AES?
159. Navedite četiri osnovna bezbednosna zahteva. Šta se podrazumeva pod pojmom POVERLJIVOST?
160. Navedite četiri osnovna bezbednosna zahteva. Šta se podrazumeva pod pojmom INTEGRITET?
161. Navedite četiri osnovna bezbednosna zahteva. Šta se podrazumeva pod pojmom PROVERA AUTENTIČNOSTI?
162. Navedite četiri osnovna bezbednosna zahteva. Šta se podrazumeva pod pojmom NEPORECIVOST?
163. Od kojih elemenata zavisi snaga šifriranja? Obrazložite na koji način DUŽINA KLJUČA utiče na snagu šifriranja.
164. Od kojih elemenata zavisi snaga šifriranja? Obrazložite na koji način NAČIN RUKOVANJA KLJUČEM utiče na snagu šifriranja.
165. Od kojih elemenata zavisi snaga šifriranja? Obrazložite na koji način PRIRODA ALGORITMA ZA ŠIFRIRANJE utiče na snagu šifriranja.
166. Šta se podrazumeva pod pojmom HEŠIRANJE?
167. Na čemu se zasniva RSA kriptografski sistem?
168. U koju kategoriju kriptografskih sistema spada RSA?
169. U koju kategoriju kriptografskih sistema spada IDEA? Na čemu se zasniva snaga ovog kriptografskog sistema?
170. Šta predstavlja digitalni potpis?
171. Šta se obično koristi za formiranje digitalnog potpisa?
172. Šta predstavlja digitalni sertifikat?