Predmety štátnej skúšky v inžinierskych študijných programoch

Informačné systémy

5IZ1H2 Štátna skúška

Problémové okruhy predmetov štátnej skúšky

Otázky na štátnej skúške sú z oblasti očakavaných znalostí inžiniera z povinných predmetov študijného program a mali by mať vzťah k záverečnej práci. Otázky môžu byť aj zo znalostí obsiahnutých v absolvovaných povinne voliteľných predmetoch.

1. **Algoritmy a údajové štruktúry**
   - Efektívne využívanie údajových štruktúr pri návrhu aplikácií.
   - Vyhľadávacie stromy a ich implementácia.
   - Pokročilé implementácie prioritného frontu.
   - Organizácia externých pamätí a súborov na externých médiách. (Sekvenčný súbor. Súbory s priamym prístupom. Štruktúra heap file, hešovanie. Indexové štruktúry.)
   - Efektívne triedenie dát v súboroch.
   - Jednorozmerné a viacrozmerné vyhľadávanie a štruktúry podporujúce vyhľadávanie.
   - Implementácia grafov.
   - Vyhľadávanie v texte.
   - Komprimačné algoritmy.
   - Algoritmy interného triedenia.
2. **Pokročilé databázové systémy**
   - Relačné DBS.
   - Objekty v DBS.
   - Jazyky a DBS (XML, SQL a PL/SQL).
   - Transakčné spracovanie a paralelizmus v DBS.
   - Distribuované spracovanie dát.
3. **Komunikačné technológie**
   - Vývoj v oblasti sieťových architektúr (klient/server a Peer-to-Peer), ekonomické a technické predpoklady pre Äll-IP"siete. Vrstvový model IP sietí.
   - Protokol IPv6 ako nástupca IPv4. Aspekty prepojenia IPv6 a IPv4 sveta.
   - Základy programovania sieťových aplikácií - TCP/IP sockety.
   - Bezpečnosť IP sietí. Princípy, úlohy a funkcie zabezpečenia sietí (integrita, autenticita, šifrovanie).
   - Bezpečnosť a zabezpečenie v TCP/IP architektúre - aplikácia po vrstvách. Zabezpečenie aplikačnej vrstvy (HTTPS). Zabezpečenie transportnej vrstvy (SSL/TLS). Zabezpečenie sieťovej vrstvy IP (IPsec). Zabezpečenie linkovej vrstvy (WiFi, EAP/EAPOL, MACsec). Prevádzková bezpečnosť (FW a IDS).
   - Služby IP sietí. Multimédia v IP sieťach a IMP protokoly. Multicast a skupinová komunikácia.
   - Prístupové siete.
   - Vývojové trendy (IMS/SDN).

4. **Optimalizácia sietí**

   - Úloha návrhu štruktúry distribučného systému, model, prostriedky riešenia, úloha odberných dní.
   - Úloha okružných jázd, úplná úloha návrhu distribučného systému, dekompozícia úlohy, model dopravnej siete.
   - Verejné a súkromné obslužné systémy.
   - Primárne a duálne heuristiky.
   - Metaheuristiky.
   - Harmonogramy dodávok a optimalizácia odberných dní.
   - Riešenie úloh okružných jázd. Metódy riešenia úlohy obsluhy úsekov dopravnej siete. Špeciálne heuristiky pre riešenie úloh okružných jázd.
   - Časové rozvrhy.

5. **Architektúry informačných systémov**

   - Informačné systémy a softvér.
   - Metodiky vývoja a riadenie projektov IS.
   - Systems and software engineering, Norma ISO/IEC/IEEE 42010:2011.
   - Modelom riadený vývoj IS.
   - Biznis architektúra - analýza požiadaviek, biznis procesy.
   - Špecifikácia požiadaviek na IS.
   - Softvérová architektúra.
   - Finalizácia vývoja informačných systémov.
   - Meranie výkonnosti informačných systémov.

6. **Diskrétna simulácia**

   - Generátory náhodných čísiel. Testovanie generátorov náhodných čísiel. Generovanie náhodných veličín.
   - Algoritmizácia simulačných modelov. Implementácia metódy plánovania udalostí a metódy snímania aktivít.
   - Kombinovaná (diskrétne-spojitá) simulácia. Animácia v simulácií.
   - Agentovo orientované architektúry simulačných modelov. Architektúra ABAsim.
   - Modelovanie komplexných systémov s využitím systémovej dynamiky. Nástroje pre modelovanie pomocou SD.
   - Distribuovaná simulácia. Konzervatívne metódy synchronizácie distribuovaných simulačných modelov. Optimistické metódy synchronizácie distribuovaných simulačných modelov.
   - Petriho siete. Využitie v modelovaní a simulácii.
   - Návrh a implementácia rozsiahlych generických simulačných modelov.

7. **Teória informácie**

   - Elementárna a axiomatická definícia informácie.
   - Informácia ako funkcia pravdepodobnosti.
   - Entropia ako stredná hodnota diskrétnej náhodnej premennej. Axiomatická definícia entropie vlastnosti entropie, podmienená entropia.
   - Zdroje informácie. Stacionárny a nezávislý zdroj, vlastnosti zdrojov, entropia zdroja.
   - Kódovanie. Blokové kódy. Prefixové kódy. Kraftova a Mac Millanova nerovnosť. Huffmanove kódovanie a kompresia správ.

- Kódy objavujúce chyby. Elementárne metódy objavovania chýb. Kódy s kontrolným znakom nad grupou. Kódy objavujúce chyby. Lineárne kódy, Hammingove a Golayove kódy.
- Prenosový kanál, kapacita kanála. Ergodicita, Shannonove vety o kapacite kanála.

8. **Databázy a získavanie znalostí**

- Algoritmy zoskupovania.
- Štatistické techniky.
- Vizualizačné techniky. Prehľad techník a porovnanie s učiacimi sa systémami.
- Čistenie a transformácia dát, testy atribútov, analýza chýb.
- Rozhodovacie stromy. Rozhodovacie pravidlá, konverzia pravidiel do rozhodovacích stromov a späť. Algoritmy generovania pravidiel.
- Algoritmy vyhľadávania.

9. **Kryptografia a bezpečnosť**

- Význam kryptografie a všeobecný model šifrovacieho systému.
- Model jazyka a šifrovacie kanála. Informácia. Entropia zdroja. Základné štatistické charakteristiky zdroja.
- Klasická kryptografia. Monoalfabetické a polyalfabetické šifry. Kryptoanalýza a základné typy útokov.
- Perfektné šifrovanie – One-Time Pad.
- Kryptografia pomocou posuvných registrov.
- Typy prúdových šifier – Stream Ciphers.
- Symetrická kryptografia. Kryptosystémy Feistelovho typu DES, GOST.
- Iné typy kryptosystémov so symetrickými kľúčmi – IDEA. Diffie - Helmannova výmena kľúčov.
- Kryptografia s verejným kľúčom. Jednosmerné funkcie. RSA – algoritmus.
- Hashovacie algoritmy.
- Kryptografické protokoly. Digitálny podpis, autentifikácia, identifikácia.
- Ukážka konkrétneho kryptosystému. Kryptografický protokol SSL.
- Mechanické šifrovacie a dešifrovacie stroje - Enigma.